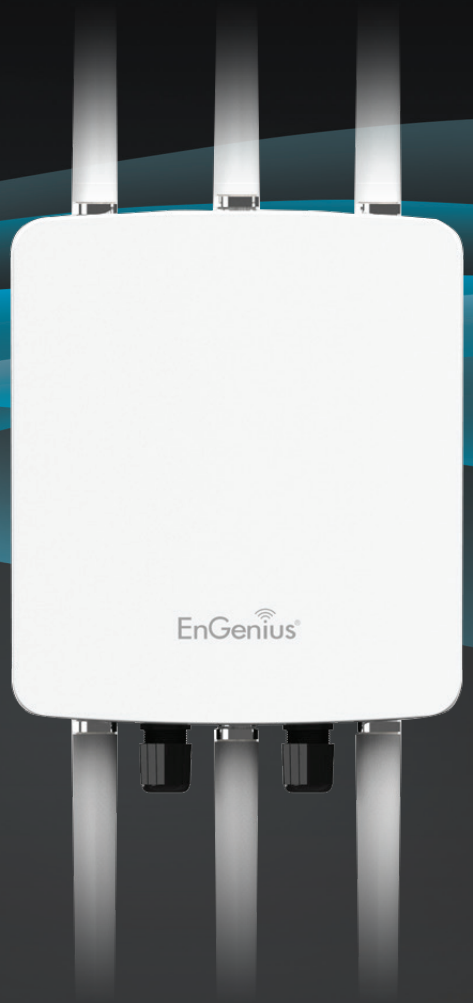
EnGenius

Business Solutions

User Manual



ENH900EXT
version 1.0

Dual Band Long Range Wireless N900 Outdoor Access Point

IMPORTANT

To install this Access Point please refer to the
Quick Installation Guide included in the product packaging.

Table of Contents

Chapter 1 Product Overview..... 4
- Key Features/Introduction..... 5
- System Requirements..... 6
- Package Contents..... 7
- Technical Specifications..... 8
- Physical Interface..... 10

Chapter 2 Before You Begin..... 11
- Computer Settings..... 12
- Hardware Installation..... 15
- Mounting the ENH900EXT..... 16

Chapter 3 Configuring Your Access Point..... 18
- Default Settings./Web Configuration..... 19

Chapter 4 Building a Wireless Network..... 20
- Access Point Mode..... 21
- WDS AP Mode..... 23
- WDS Bridge Mode..... 24
- WDS Station Mode..... 25
- AP Mesh Mode..... 26
- Mesh Only Mode..... 27

Chapter 5 Status..... 28
- Main Status..... 29
- Connection..... 32

Chapter 6 Network 34
- Basic IP Settings..... 35
- Spanning Tree Protocol Setting..... 36

Chapter 7 2.4 GHz/5 GHz Wireless..... 37
- Wireless Settings..... 38
- 2.4 GHz/5 GHz Wireless Network..... 39
- 2.4GHz/5 GHz SSID Profile..... 41
- Wireless Security..... 42
- Wireless MAC Filtering..... 43
- Wireless Advanced..... 44
- WPS Mixed-Enterprise: AP/WDS AP Mode..... 45
- WDS Link Settings..... 46
- 2.4 GHz Mesh Link Settings..... 47
- Guest Network Settings..... 48

Chapter 8 Management 49
- Management VLAN Settings..... 50
- Wi-Fi Multi Media..... 51
- Advanced Settings..... 52
- CLI Settings/Email Alert..... 53
- Time Zone..... 55
- Auto Reboot Settings..... 56
- Wi-Fi Scheduler..... 57
- Tools..... 58
- Account/Firmware..... 60
- Backup/Restore 61
- Log..... 62
- Logout/Reset..... 63

Glossary..... 64

Appendix..... 71
- FCC Interference Statement..... 72
- CE Interference Statement..... 73

Chapter 1

Product Overview

Introduction

Key Features

- Up to 29 dBm transmit power enabling long range connectivity
- Supports IEEE802.11a/b/g/n wireless standards with up to 450 Mbps data rate on each band.
- Three detachable 5 dBi 2.4 GHz Omni-directional antennas
- Three detachable 7 dBi 5 GHz Omni-directional antennas
- Mesh Supported (2.4 Ghz)
- Can be used with included power adapter or via PoE with PoE 802.3at - capable switches or injectors
- Dual Band/Three Stream
- Band Steering shifts dual band clients to 5 GHz for better throughput performance
- Secured Guest Network option available

Introduction

The ENH900EXT is a high-powered, long-range 3x3 Dual-Band Wireless 802.11a/b/g/n Outdoor Access Point with speeds up to 450 Mbps on both its high-powered 2.4 GHz and 5 GHz radios. It can be configured as an: Access Point, or WDS (AP, Station & Bridge). The ENH900EXT is designed to operate in a variety of outdoor environments. Its high-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that don't have the range and reach to connect to a growing number of wireless users who wish to connect to a business network. The ENH900EXT supports the 2.4 GHz frequency band under 802.11 b/g/n mode while at the same time providing the 5 GHz band for communicating to and from other 5 GHz capable computers, tablets or smart phones or transferring files. Several ENH900EXTs can be deployed

Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment, and mix of devices in the network. Features and specifications subject to change without notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright © 2014 EnGenius Technologies, Inc. All rights reserved.

in a campus setting using the 5 GHz band as a backhaul to provide multiple 2.4 GHz wireless cells for computers or mobile devices in common outdoor areas.

The ENH900EXT is easy to install in virtually any location with its included PoE (Power over Ethernet) injector for quick outdoor installation. The ENH900EXT enables network administrators to control its transmit power and features settings for selecting narrow bandwidth and traffic shaping. The ENH900EXT also supports wireless encryption including Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) Encryption and IEEE 802.1X with RADIUS.

System Requirements

The following are the Minimum System Requirements in order to configure the device.

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7), Mac OS, or Linux-based operating systems
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or another similar browser application)

Package Contents

The ENH900EXT package contains the following items:*

- ENH900EXT Access Point
- 3 detachable 5 dBi 2.4 GHz Omni-directional Antenna
- 3 detachable 7 dBi 5 GHz Omni-directional Antenna
- Power Adapter (48V/0.8A)
- PoE Injector (EPE-48GR)
- Grounding Cable
- Pole Mount Bracket
- Wall Mount Base
- Mounting Screw Set
- Quick Installation Guide
- Technical Support Card

*(all items must be in package to issue a refund):

Technical Specifications

Standard:
IEEE802.11a/n on 5 GHz
IEEE802.11b/g/n on 2.4 GHz
IEEE802.3at

Antenna
6 External N-type Antenna
- 3 x detachable 5 dBi 2.4 GHz Omni-directional Antennas
- 3 x detachable 7 dBi 5 GHz Omni-directional Antennas

Physical Interface
2 x 10/100/1000 Gigabit Ethernet Port with PoE support
- LAN1 Port: IEEE802.3at PoE Input
- LAN2 Port: IEEE802.3af PoE Output
- Both Ethernet Ports support Surge Protection to 6KV

LED Indicator
Power
LAN 1
LAN 2
2.4 GHz
5 GHz

Power Requirements
External Power Adapter, DC IN, 48V/0.8A
IEEE802.3at support

Operation Modes
Access Point
WDS
Mesh (2.4 GHz)

WDS Detail
WDS AP
WDS Bridge
WDS Station

Mesh Detail
Mesh AP
Mesh Only

Management
Auto Channel Selection
Multiple SSID: 16 SSIDs, 8 SSIDs per Radio
BSSID
SNMP V1/V2c/V3
MIB I/II, Private MIB
VLAN Tag/VLAN Pass-through
Clients Statistics
Save Configuration as User Default
Fast Roaming
E-Mail Alert
RADIUS Accounting
Guest Network

Control
CLI Supported
Distance Control (Ack Timeout)
802.1X Supplicant (CB Mode)
Multicast Supported
Auto Reboot
Obey Regulatory Power

Security

WEP Encryption - 64/128/152 bit
WPA/WPA2 Personal (WPA-PSK using TKIP or AES)
WPA/WPA2 Enterprise (WPA-PSK using TKIP or AES)
Hides SSID in beacons
MAC address filtering, up to 50 MACs
Wireless STA (Client) connection list
Https Support
SSH Support

QoS (Quality of Service)

Complaint with IEEE 802.11e standard

Physical/Environment Conditions

Operating:

Temperature: -4 °F to 158 °F (-20 °C to 70 °C)
Humidity (non-condensing): 90% or less

Storage:

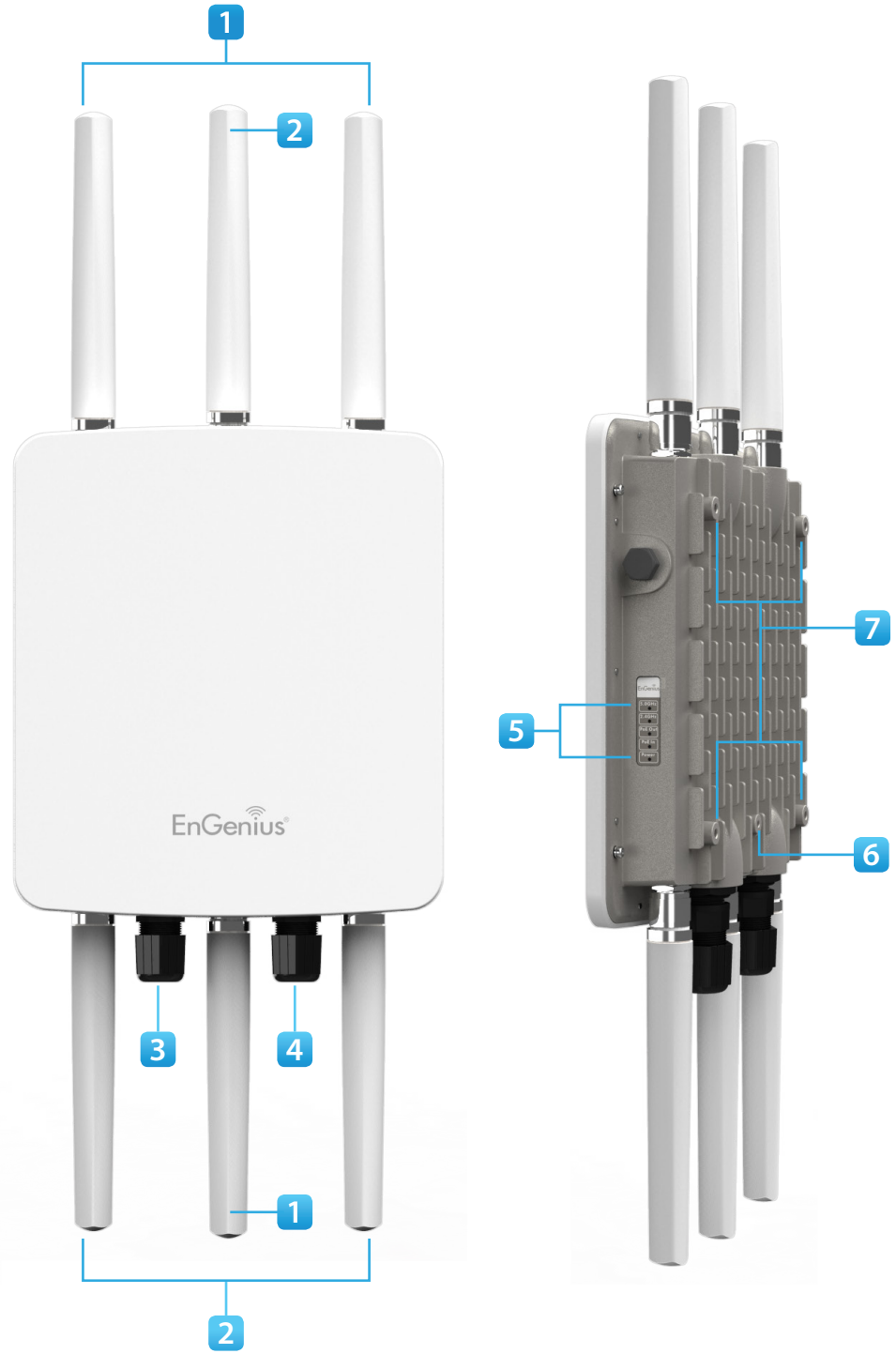
Temperature: -22 °F to 176 °F (-30 °C to 80 °C)
Humidity (non-condensing): 90% or less

RF Specification (Aggregated Value)

Channel	Data Rate	Tx Power	Rx Sensitivity
802.11b 2.4GHz	1Mbps	29	-96
	2Mbps	29	-95
	5.5Mbps	29	-93
	11Mbps	29	-92
802.11g 2.4GHz	6Mbps	28	-94
	54Mbps	25	-75
802.11a 5GHz	6Mbps	29	-94
	54Mbps	24	-75
802.11n HT20 2.4GHzx	MCS0/ 8 / 16	29	-95
	MCS7 / 15 / 23	24	-70
802.11n HT40 2.4GHz	MCS0/ 8 / 16	29	-94
	MCS7 / 15 / 23	24	-69
802.11n HT20 5GHz	MCS0/ 8 / 16	27	-95
	MCS7 / 15 / 23	23	-70
802.11n HT40 5GHz	MCS0/ 8 / 16	27	-94
	MCS7 / 15 / 23	23	-69
802.11ac HT20 5GHz	MCS0	-	-
	MCS8	-	-
802.11ac HT40 5GHz	MCS0	-	-
	MCS9	-	-
802.11ac HT80 5GHz	MCS0	-	-
	MCS9	-	-

Physical Interface

Dimensions and Weights
Length: 11.22”
Width: 8.58”
Depth: 2.1”
Weight: 4.17 lbs



1 **2.4 GHz Antennas:** Detachable 5 dBi 2.4 GHz Omni-directional
2 **5 GHz Antennas** Detachable 7 dBi 5 GHz Omni-directional
3 **LAN Port 1 (802.3at PoE Input)**: Ethernet port for RJ-45 cable.
4 **LAN Port 2 (802.3af PSE Output):** Ethernet port for RJ-45 cable.
5 **LED Indicators:** LED lights for Power, LAN Port 1, LAN Port 2, 2.4 GHz Connection and 5 GHz Connection.
6 **Ground**
7 **Mounting Holes:** Using the provided hardware, the ENH900EXT can be attached to a wall or pole.

Chapter 2

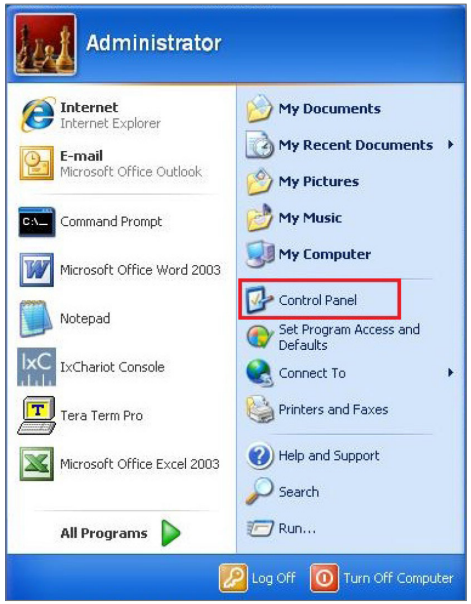
Before You Begin

Computer Settings

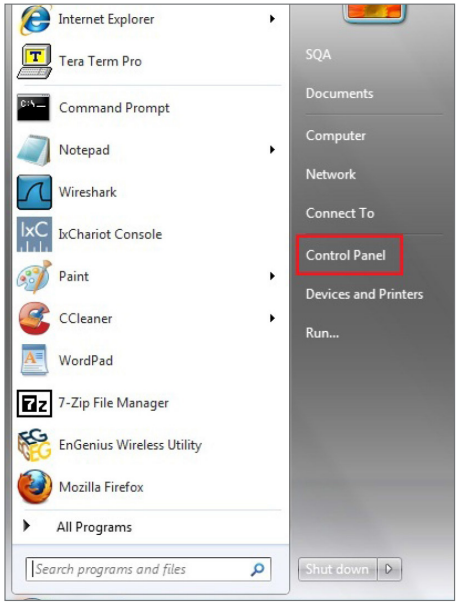
Windows XP/Windows 7

In order to use the ENH900EXT, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

1. Click the **Start** button and open the **Control Panel**.



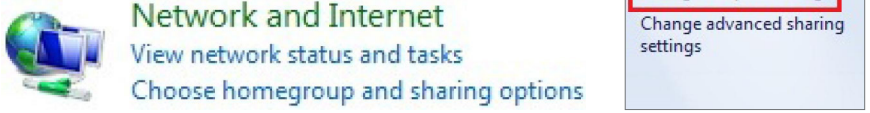
Windows XP



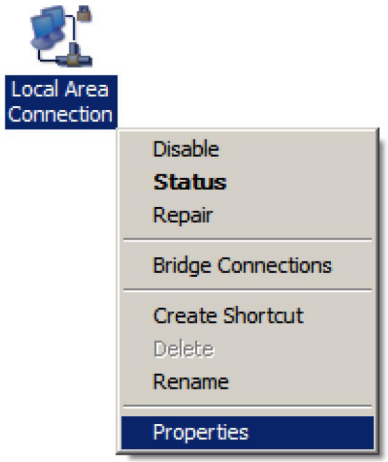
Windows 7

2a. In **Windows XP,** click **Network Connections.**

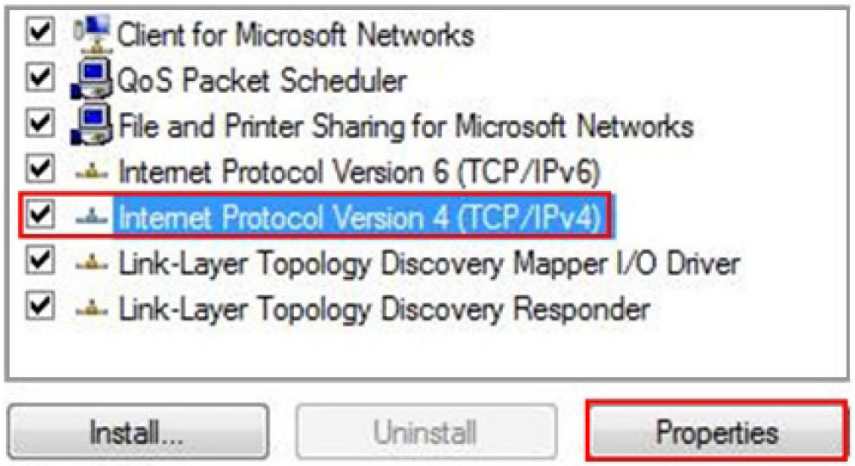
2b. In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet** section, then select **Change adapter settings.**



3. Right click on **Local Area Connection** and select **Properties.**



4. Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



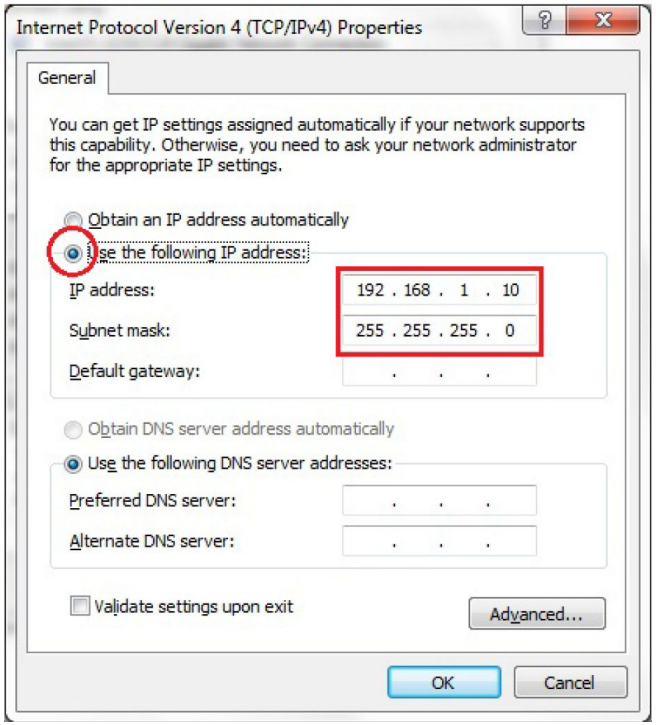
5. Select **Use the following IP address** and enter an IP address that is different from the ENH900EXTand Subnet mask, then click **OK**.

Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: ENH900EXT IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.255

PC Subnet mask: 255.255.255.0


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Apple Mac OS X

1. Go to **System Preferences** (Which can be opened in the Applications folder or selecting it in the Apple Menu).
2. Select **Network** in the **Internet & Network** section.

3. Highlight **Ethernet.**
4. In **Configure IPv4**, select **Manually.**
5. Enter an IP address that is different from the ENH900EXT and Subnet mask then press **OK.**

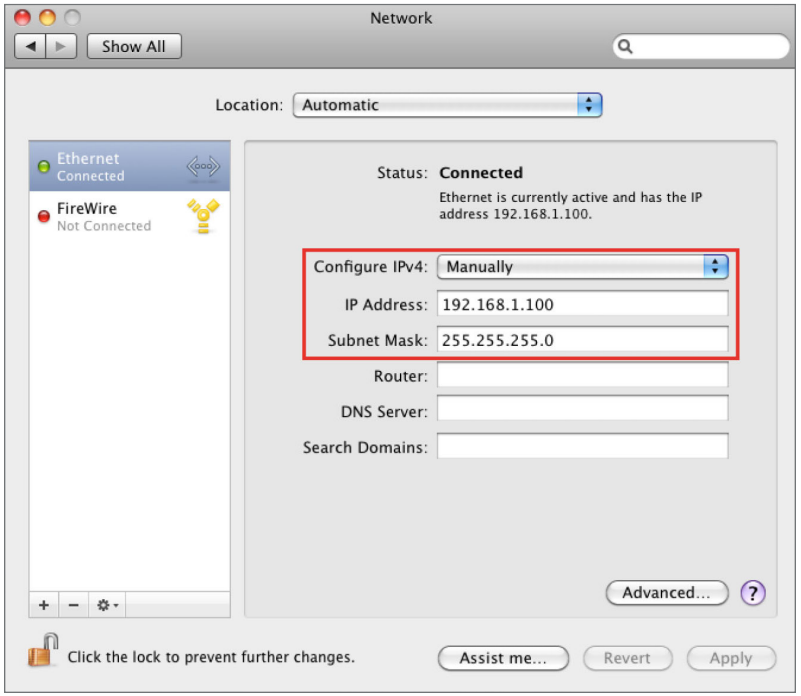
   Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

   For example: ENH900EXT IP address: 192.168.1.1

   PC IP address: 192.168.1.2 - 192.168.1.255

   PC Subnet mask: 255.255.255.0

6. Click **Apply** when done.



Hardware Installation

1. Connect one end of the Ethernet cable into the main LAN port (PoE) of the Access Point and the other end to the AP Ethernet port on the PoE injector.
2. Connect the **Power Adapter** to the **DC-IN** port of the PoE injector and plug the other end in to an electrical outlet.
3. Connect the second Ethernet cable into the **LAN port** of the PoE injector and the other end to the Ethernet port on the computer.
4. Screw on the provided antennas to the device. Once both connections are secure, verify the following:

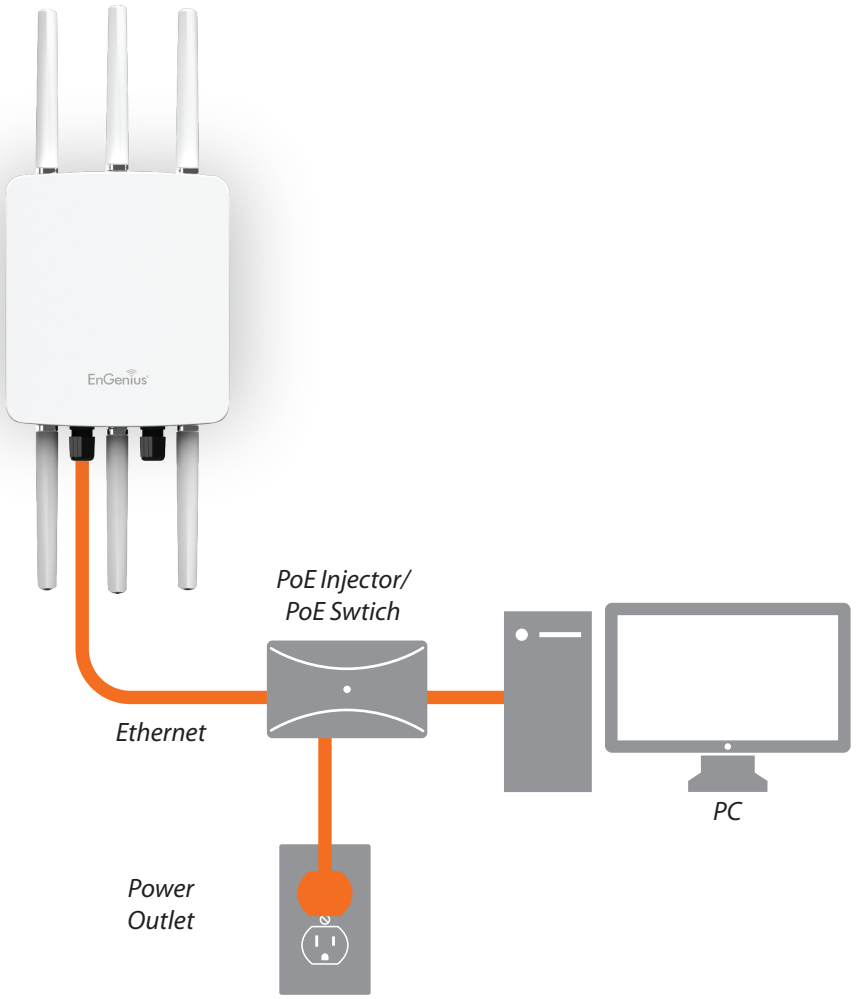
   a) Ensure that the **POWER** light is on (it will be green).

   b) Ensure that the 2.4 GHz/5 GHz WLAN light is on (it will be green for both 5 GHz and 2.4 GHz).

   c) Ensure that the LAN (Computer/ENH900EXT Connection) light is on (it will be green).

   d) Once all three lights are on, proceed to set up the Access Point using the computer.

This diagram depicts the hardware configuration.



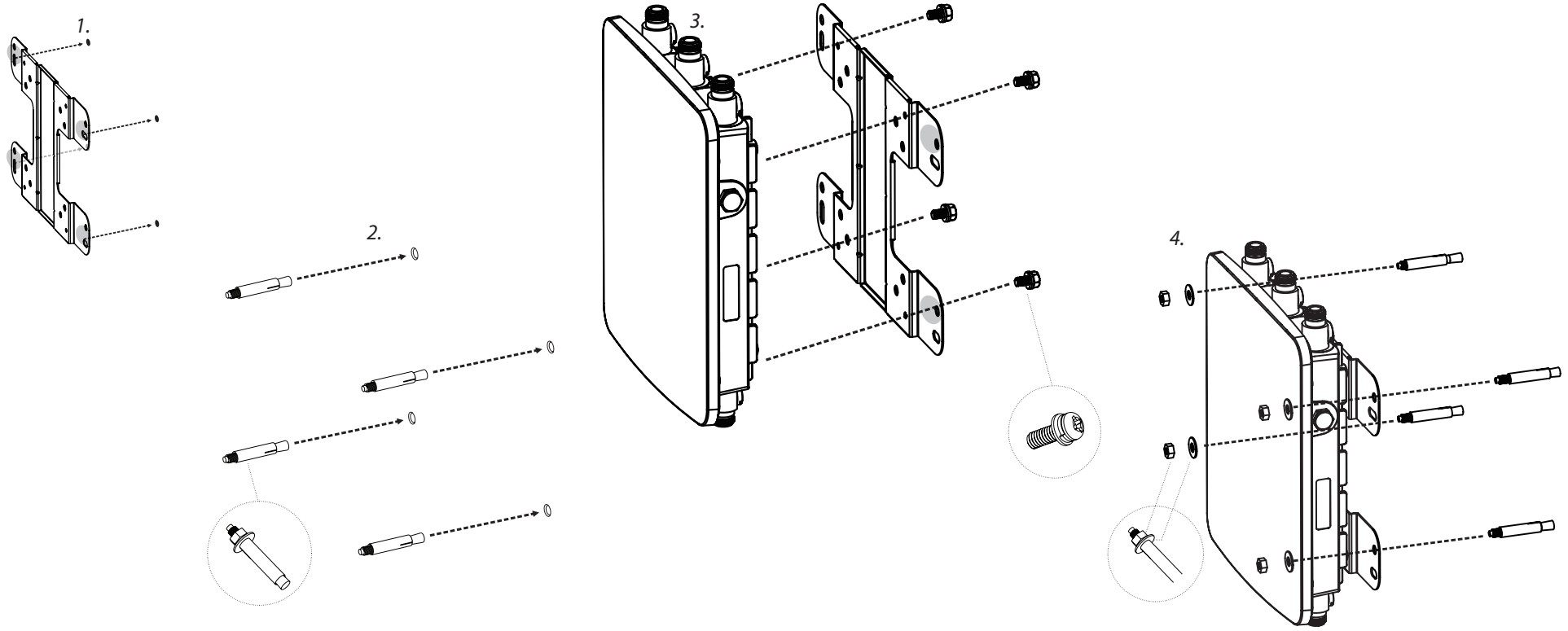
Note: The Access Point supports both IEEE 802.3at PoE (Power over Ethernet) or the included power injector. You may use either one as the power source. **Do NOT use both at the same time.**

Mounting the ENH900EXT

Using the provided hardware, the ENH900EXT can be attached to a wall or a pole.

To attach the ENH900EXT to a wall using wall mounting kit.

1. Mark the four locations of the mounting holes on the flat mounting surface.
2. Drill a 37 mm deep 8 mm hole in the markings and hammer the bolts into the openings.
3. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
4. Tighten the flat washers to secure the bracket to the mounting surface.

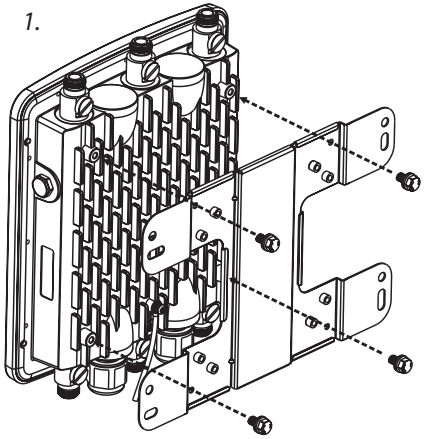


To attach the ENH900EXT to a pole using the provided pole mounting kit:

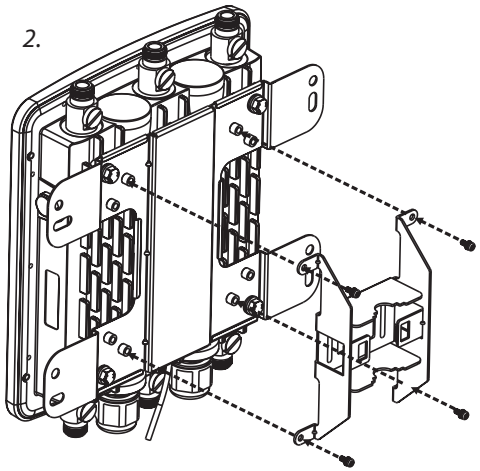
1. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
2. Drive the four round head screws to attach the Pole Mount Bracket to the bracket.
3. Thread the open end of the Pole Strap through the two tabs on the Pole Mount Bracket .
4. Lock and tighten the Pole Strap to secure the Pole Mount Bracket to the pole.

   Note: See diagram below for vertical and horizonal placements.

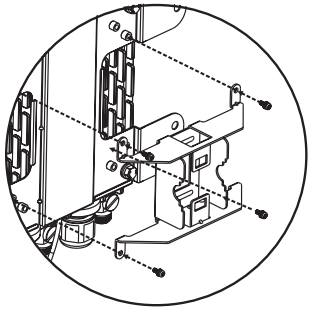
1.



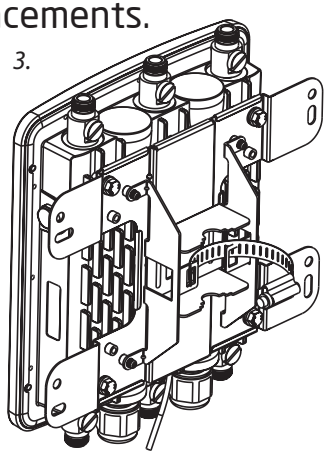
2.



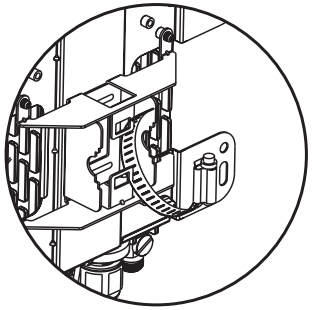
horizontal placement



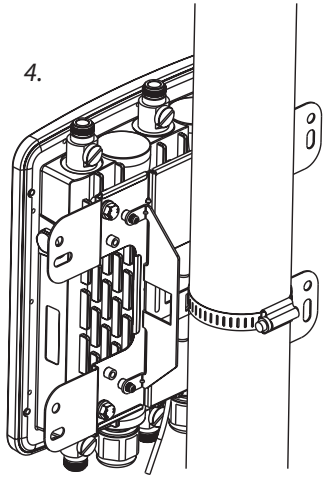
3.



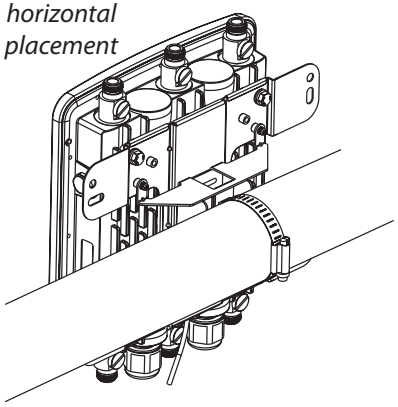
horizontal placement



4.



horizontal placement



Chapter 3

Configuring Your Access Point

Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

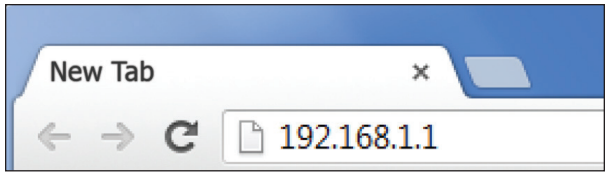
Default Settings

Please use your Ethernet port or wireless network adapter to connect the Access Point.

IP Address	192.168.1.1
Username / Password	admin / admin

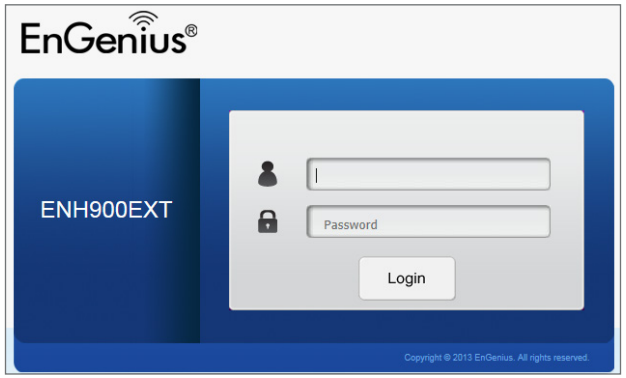
Web Configuration

1. Open a web browser (Internet Explorer/Firefox/Safari/Chrome) and enter the IP Address **http://192.168.1.1**

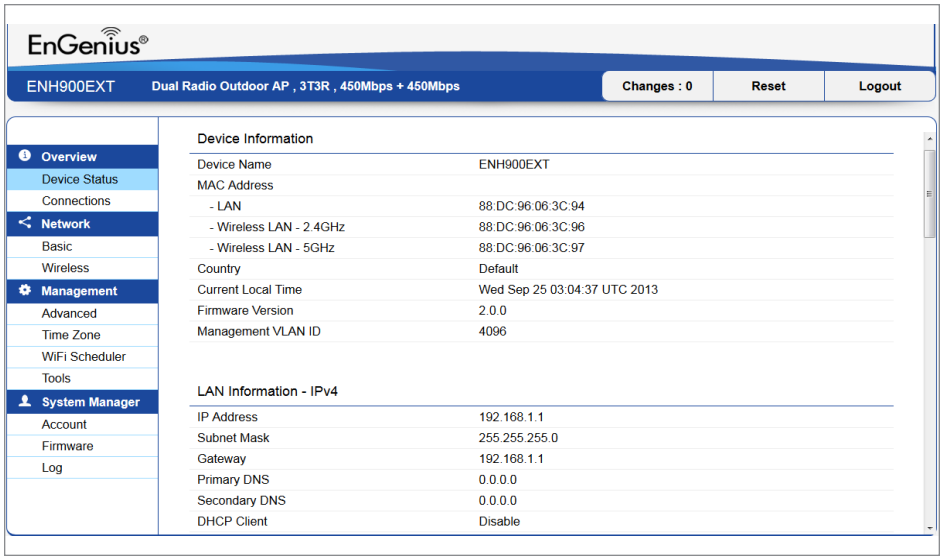


Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

2. The default username and password are **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-base configuration page.



3. If successful, you will be logged in and see the ENH900EXT User Menu.



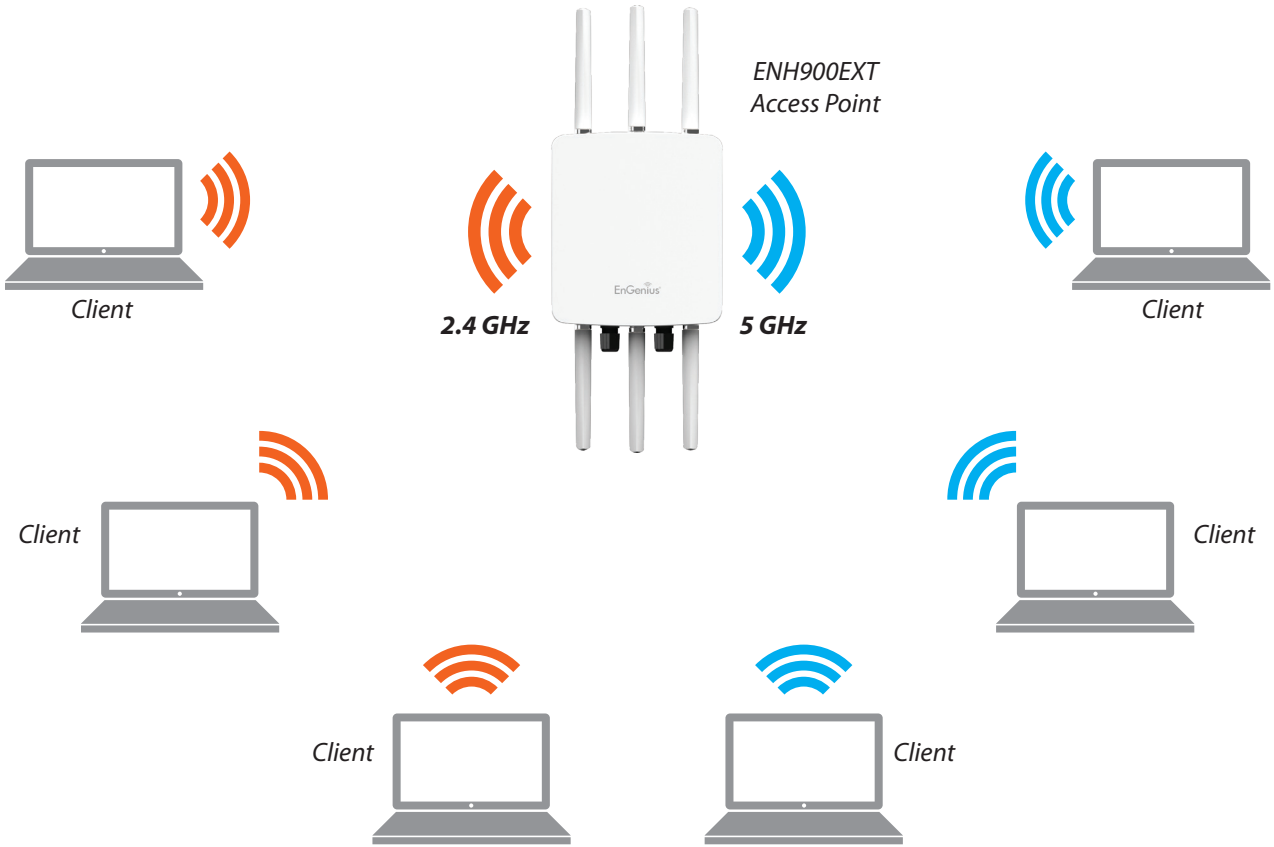
Chapter 4

Building a Wireless Network

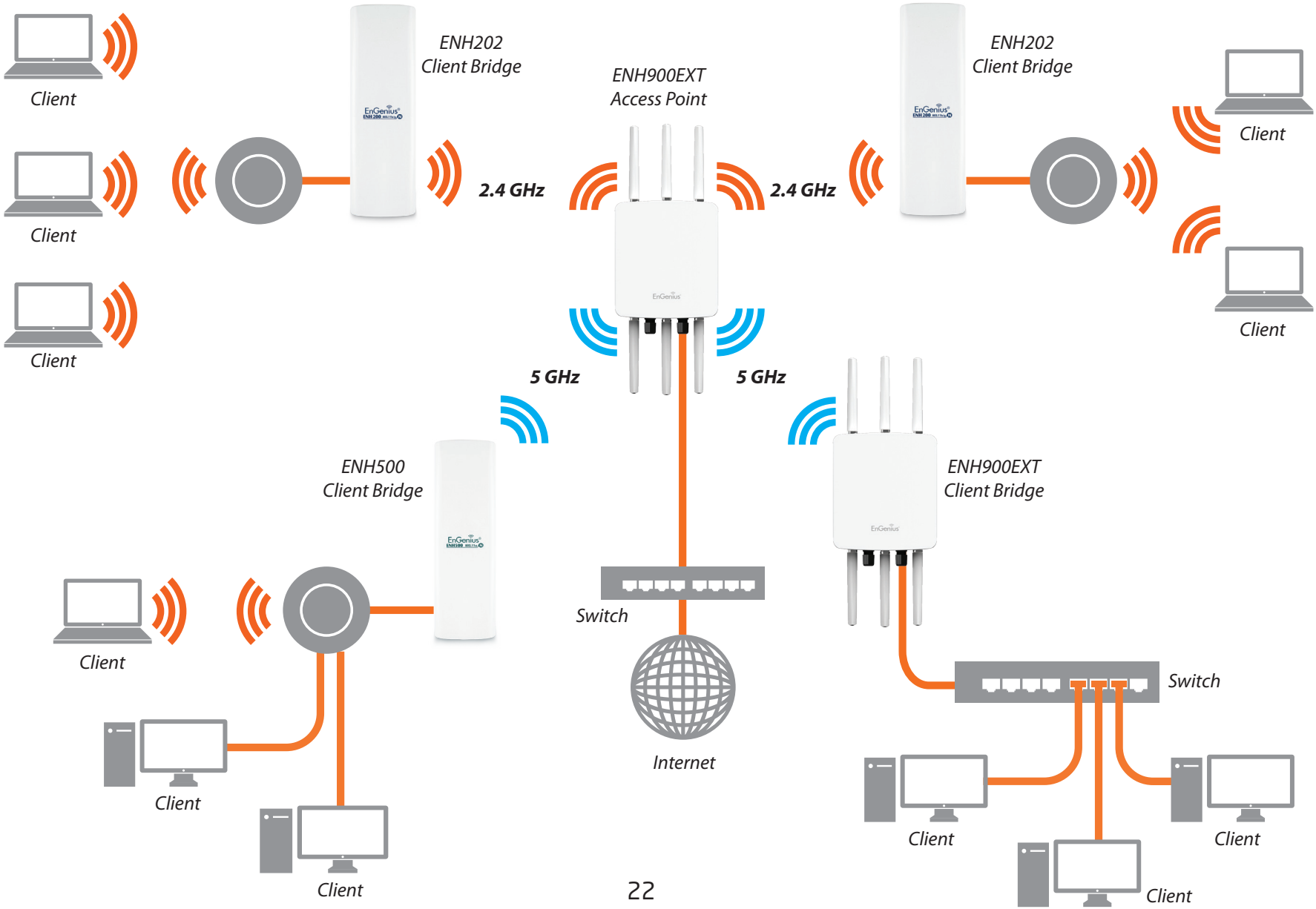
The ENH900EXT has the ability to operate in various modes. This chapter describes the operating modes of the ENH900EXT.

Access Point Mode

In Access Point Mode, ENH900EXT behaves likes a central connection for stations or clients that support IEEE 802.11a/b/g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the ENH900EXT. The ENH900EXT supports up to eight SSIDs per band at the same time for secure access.

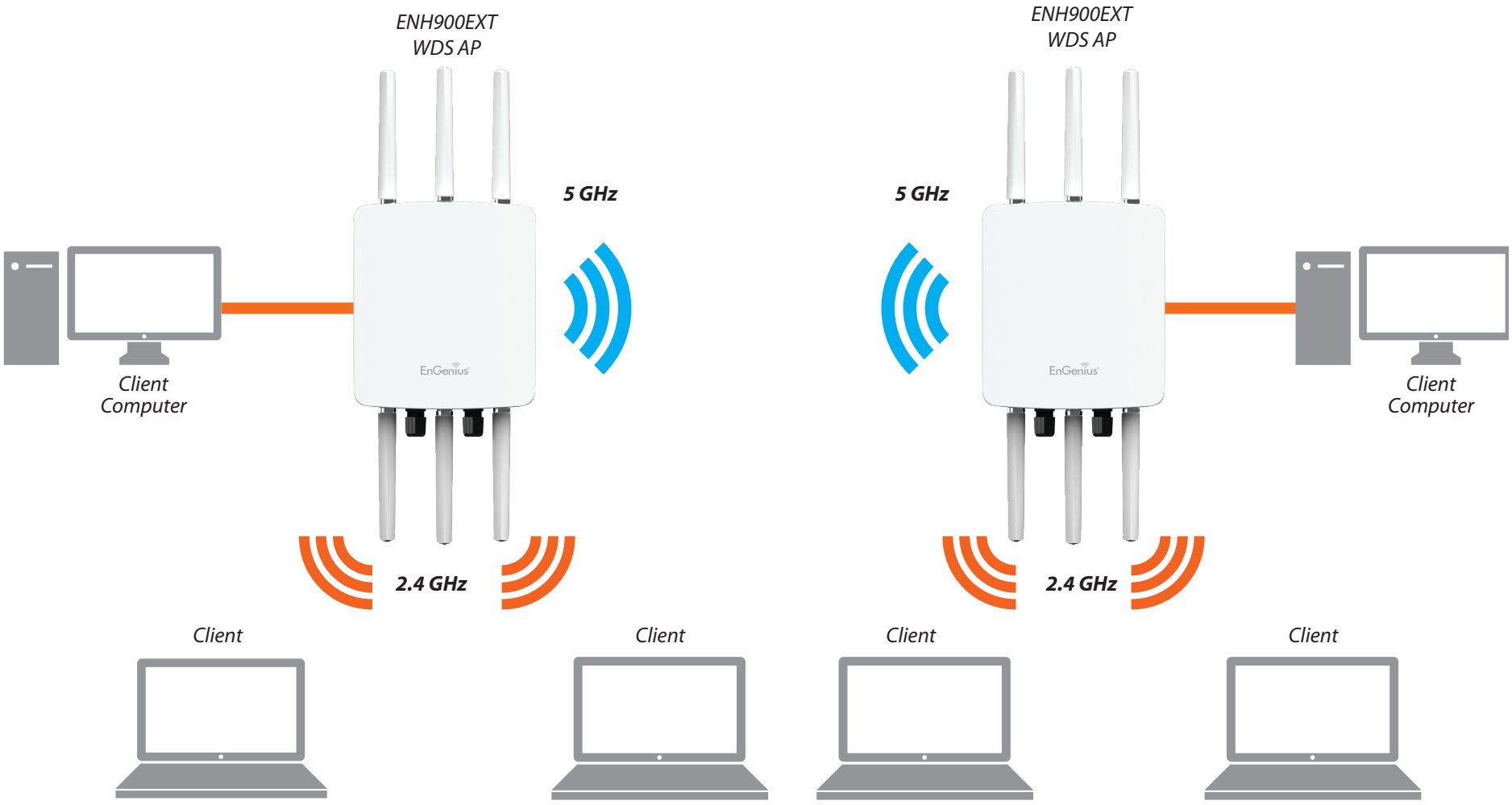


The ENH900EXT can be used as a centralized Outdoor Access Point with which other EnGenius Wireless N 2.4 or 5 GHz Outdoor Client Bridges can associate; leveraging the long-range capability of their internal high-gain directional antennas, resulting in a very cost-effective solution to expand a company network over a multiple building campus.



WDS AP Mode

The ENH900EXT also supports WDS AP mode. This operating mode allows wireless connections to the ENH900EXT using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports up to four (4) AP MAC addresses.

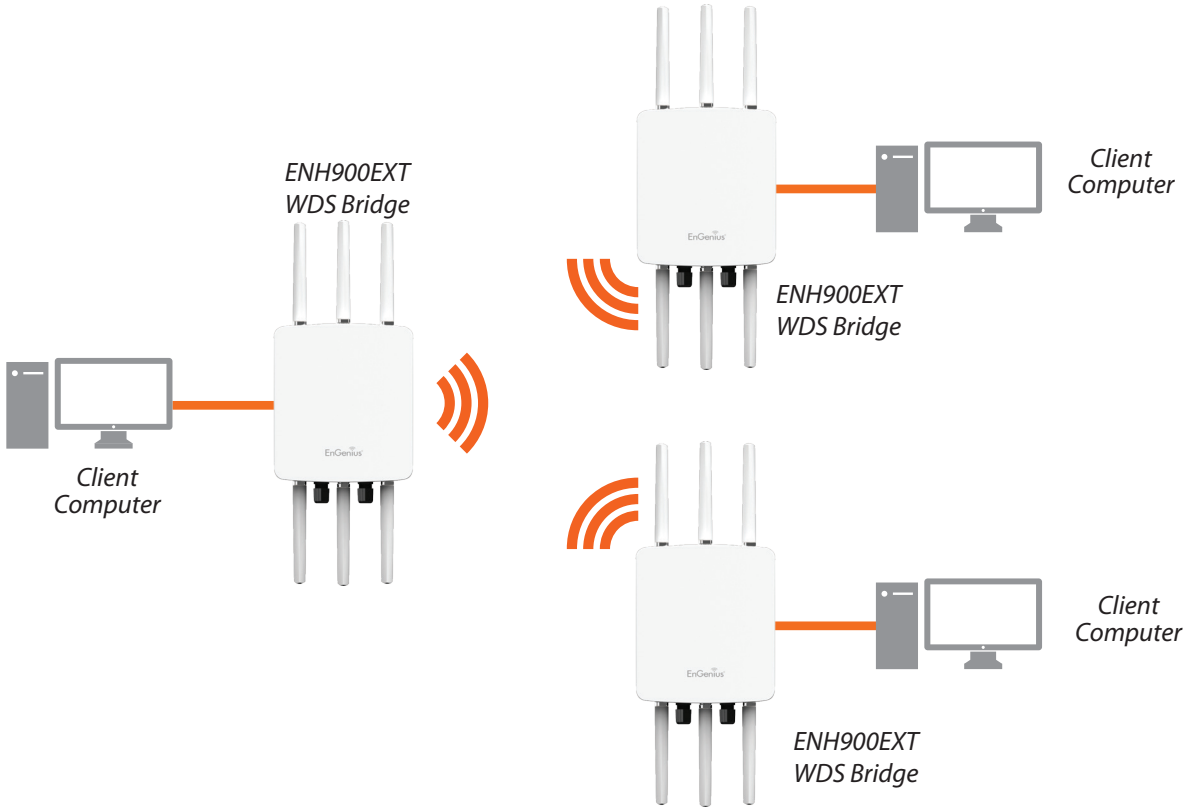


WDS Bridge Mode

In WDS Bridge Mode, the ENH900EXT can wirelessly connect different LANs by configuring the MAC address and security settings of each ENH900EXT device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the ENH900EXT to wirelessly connect two wired LANs, as shown in the following diagram.

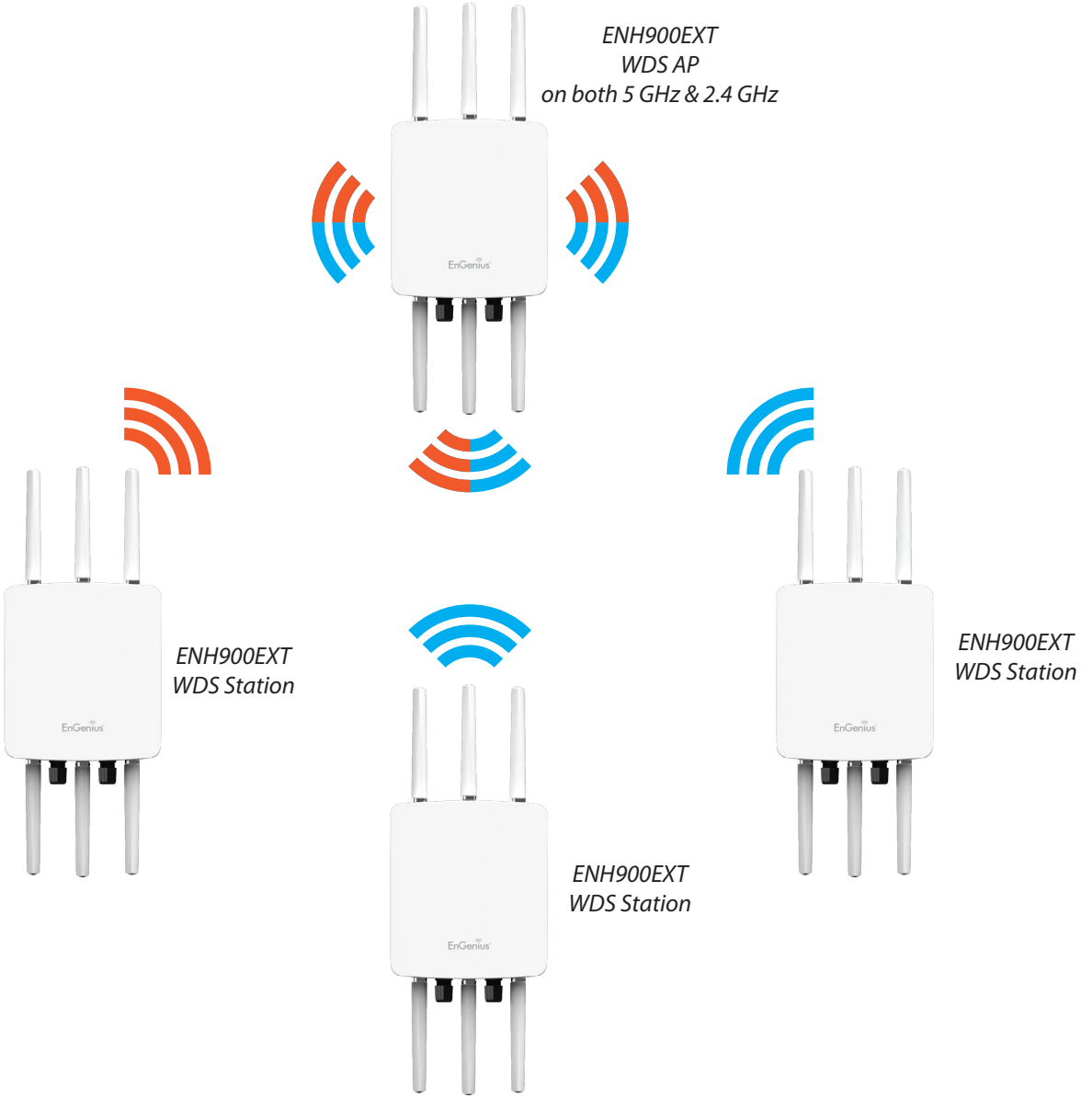
WDS Bridge Mode can establish up to four WDS links, creating a star-like network.

Note: WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. This configuration can be susceptible to generate endless network loops in your network, so it is recommended to enable the Spanning Tree function to prevent this from happening.



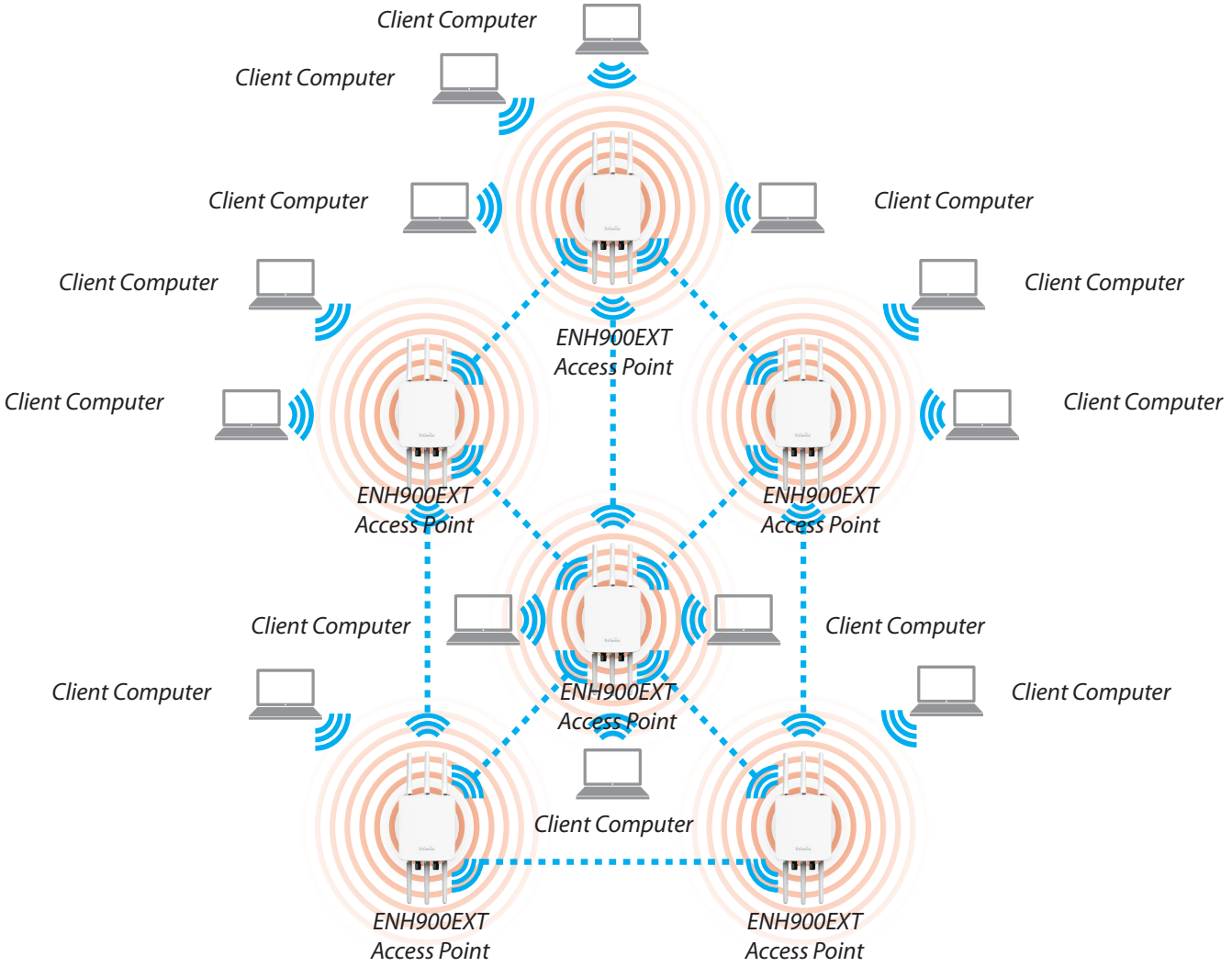
WDS Station Mode

Station mode expands the WDS by receiving a wireless signal/service and sharing it through the Ethernet port.



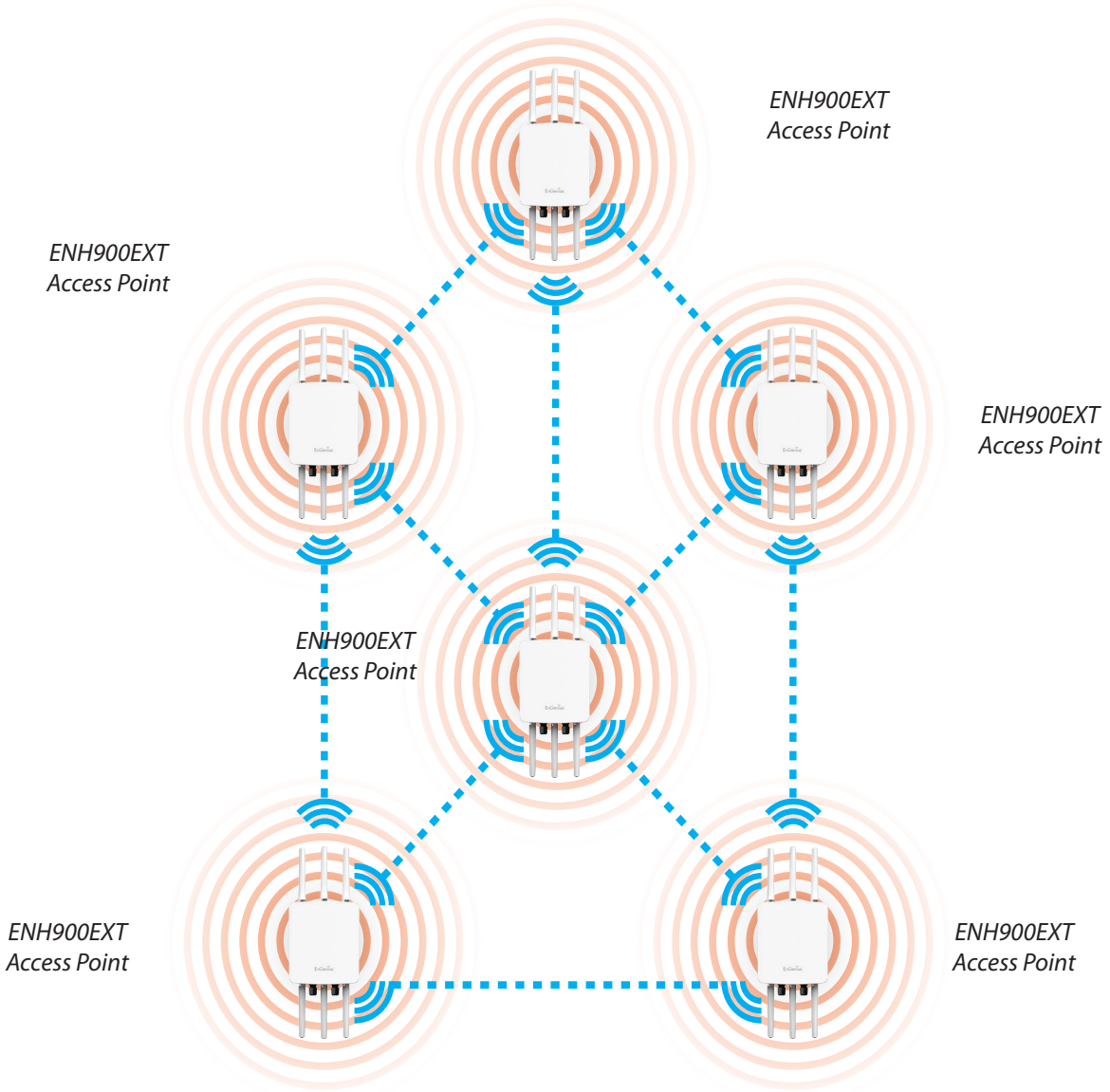
AP Mesh Mode

Under the AP Mesh mode (2.4 GHz only), the ENH900EXT can be used as the central connection hub for station or clients that support IEEE 802.11 b/g/n network. Under this mode, the ENH900EXT can be configured with the same Mesh SSID and security password in order to associate with other ENH900EXTs, as well as connect with clients under the same SSID and encryption signatures. For example, you would use one band to connect Access Points in range with Mesh mode and the other band to broadcast traffic on the network.



Mesh Only Mode

Under the Mesh-only mode, the ENH900EXT can be configured with the same Mesh SSID and security password in order to associate with other Mesh enabled ENH900EXTs, instead of connecting with clients.

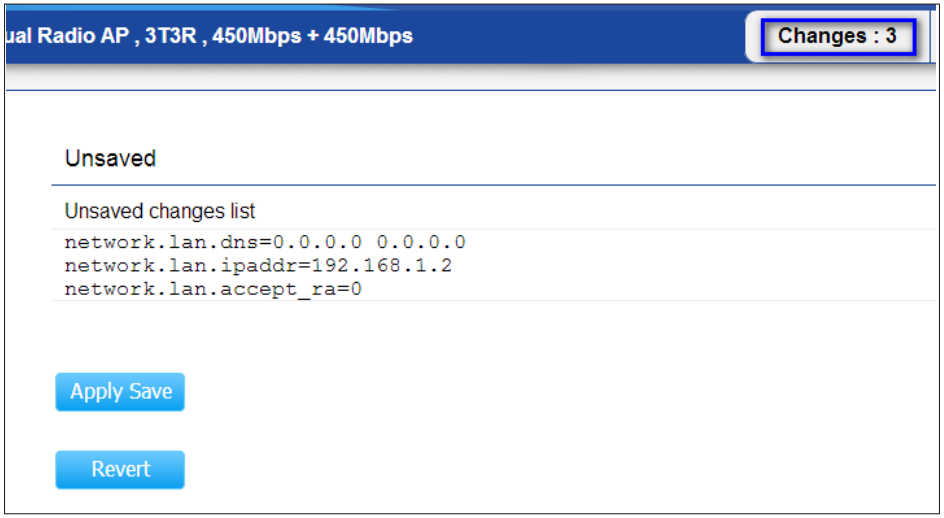


Chapter 5
Status

Main Status

Save Changes

This page lets you save and apply the settings shown under **Unsaved changes list**, or cancel the unsaved changes and revert to the previous settings that were in effect.



Device Status

Clicking the **Device Status** link under the **Overview** menu shows the status information about the current operating mode.

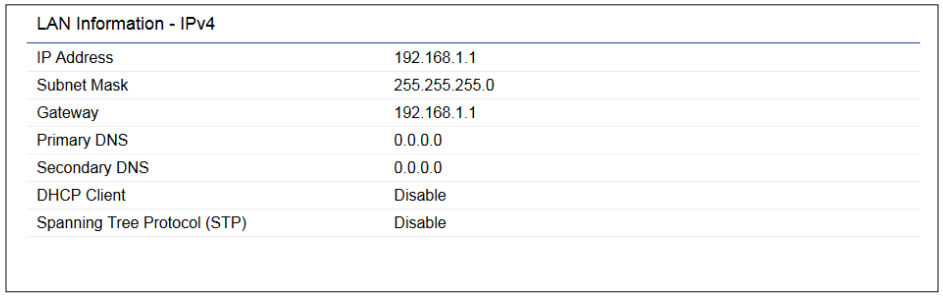
- The **Device Information** section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID

  Note: VLAN ID is only applicable in Access Point or WDS AP mode.

Device Information	
Device Name	ENH900EXT
MAC Address	
- LAN	88:DC:96:06:3C:94
- Wireless LAN - 2.4GHz	88:DC:96:06:3C:96
- Wireless LAN - 5GHz	88:DC:96:06:3C:97
Country	Default
Current Local Time	Wed Sep 25 03:04:37 UTC 2013
Firmware Version	2.0.0
Management VLAN ID	4096

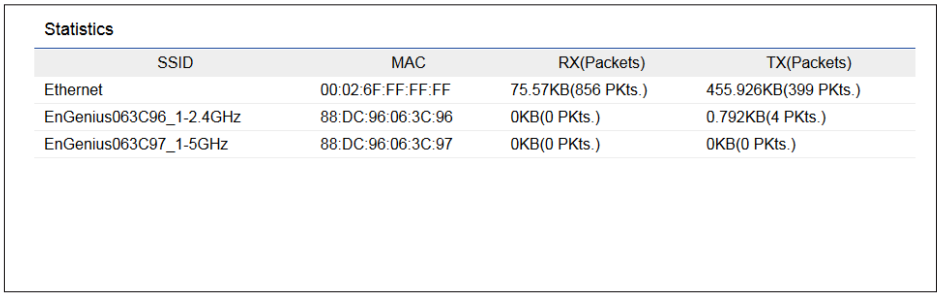
- The **LAN Information** section shows the Local Area

Network settings such as the LAN IP Address, Subnet mask, and DNS Address.



LAN Information - IPv4

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disable
Spanning Tree Protocol (STP)	Disable

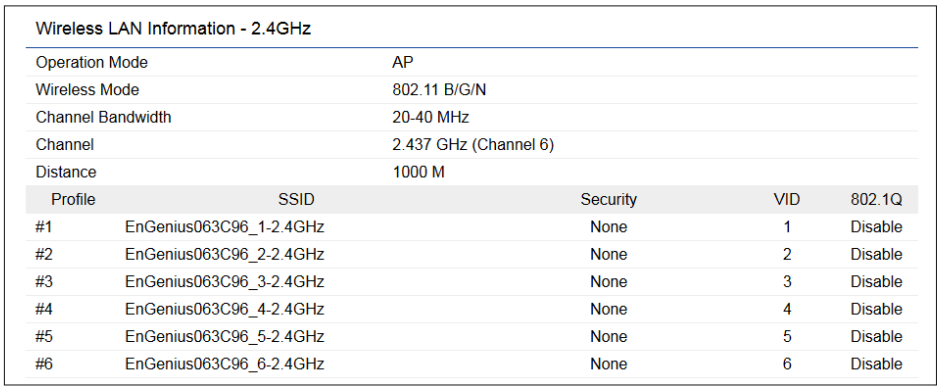


Statistics

SSID	MAC	RX(Packets)	TX(Packets)
Ethernet	00:02:6F:FF:FF:FF	75.57KB(856 PKts.)	455.926KB(399 PKts.)
EnGenius063C96_1-2.4GHz	88:DC:96:06:3C:96	0KB(0 PKts.)	0.792KB(4 PKts.)
EnGenius063C97_1-5GHz	88:DC:96:06:3C:97	0KB(0 PKts.)	0KB(0 PKts.)

- The **Wireless LAN Information 2.4 GHz/5 GHz** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the ENH900EXT supports multiple-SSIDs, information about each SSID, the ESSID, and security settings, are displayed

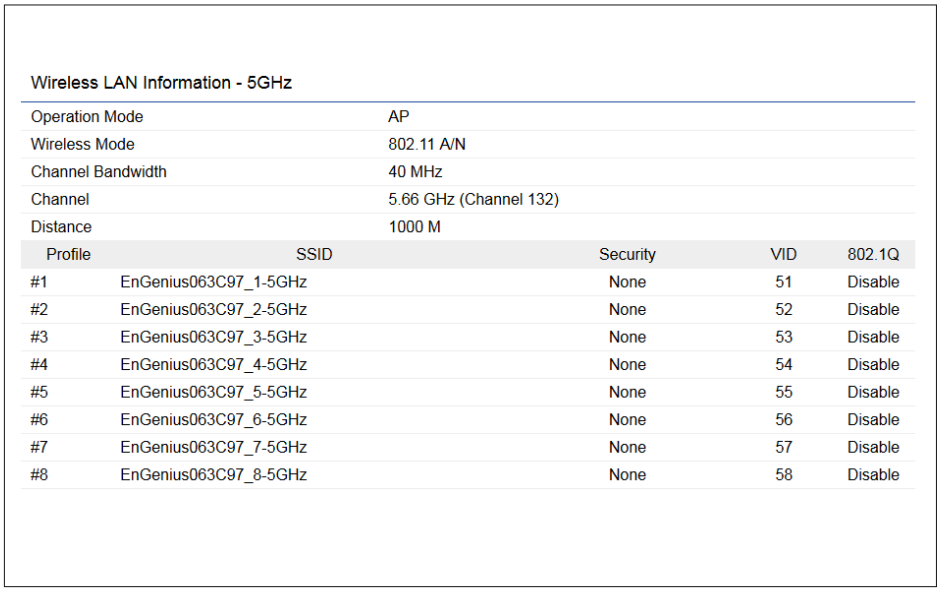
  Note: Profile Settings are only applicable in Access Point and WDS AP modes.



Wireless LAN Information - 2.4GHz

Operation Mode	AP
Wireless Mode	802.11 B/G/N
Channel Bandwidth	20-40 MHz
Channel	2.437 GHz (Channel 6)
Distance	1000 M

Profile	SSID	Security	VID	802.1Q
#1	EnGenius063C96_1-2.4GHz	None	1	Disable
#2	EnGenius063C96_2-2.4GHz	None	2	Disable
#3	EnGenius063C96_3-2.4GHz	None	3	Disable
#4	EnGenius063C96_4-2.4GHz	None	4	Disable
#5	EnGenius063C96_5-2.4GHz	None	5	Disable
#6	EnGenius063C96_6-2.4GHz	None	6	Disable



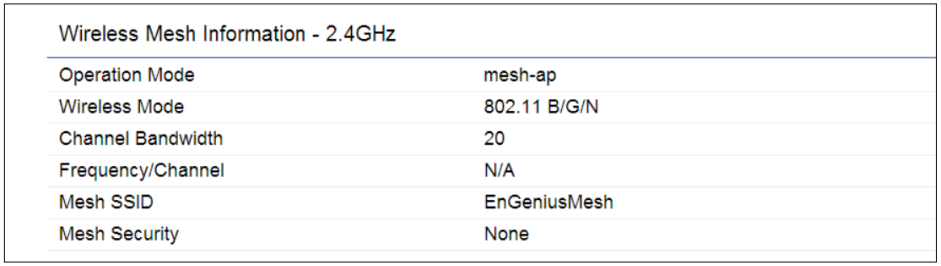
Wireless LAN Information - 5GHz

Operation Mode	AP
Wireless Mode	802.11 A/N
Channel Bandwidth	40 MHz
Channel	5.66 GHz (Channel 132)
Distance	1000 M

Profile	SSID	Security	VID	802.1Q
#1	EnGenius063C97_1-5GHz	None	51	Disable
#2	EnGenius063C97_2-5GHz	None	52	Disable
#3	EnGenius063C97_3-5GHz	None	53	Disable
#4	EnGenius063C97_4-5GHz	None	54	Disable
#5	EnGenius063C97_5-5GHz	None	55	Disable
#6	EnGenius063C97_6-5GHz	None	56	Disable
#7	EnGenius063C97_7-5GHz	None	57	Disable
#8	EnGenius063C97_8-5GHz	None	58	Disable

- The **Statistics** section shows Mac information such as SSID, MAC address, RX and TX.

- The **Wireless Mesh Information - 2.4 GHz** section shows wireless information such as Operation Mode, Wireless Mode, Channel Bandwidth, Frequency/ Channel, Mesh SSID and Mesh Security.



Wireless Mesh Information - 2.4GHz	
Operation Mode	mesh-ap
Wireless Mode	802.11 B/G/N
Channel Bandwidth	20
Frequency/Channel	N/A
Mesh SSID	EnGeniusMesh
Mesh Security	None

Connection

2.4 GHz/5 GHz Connection List

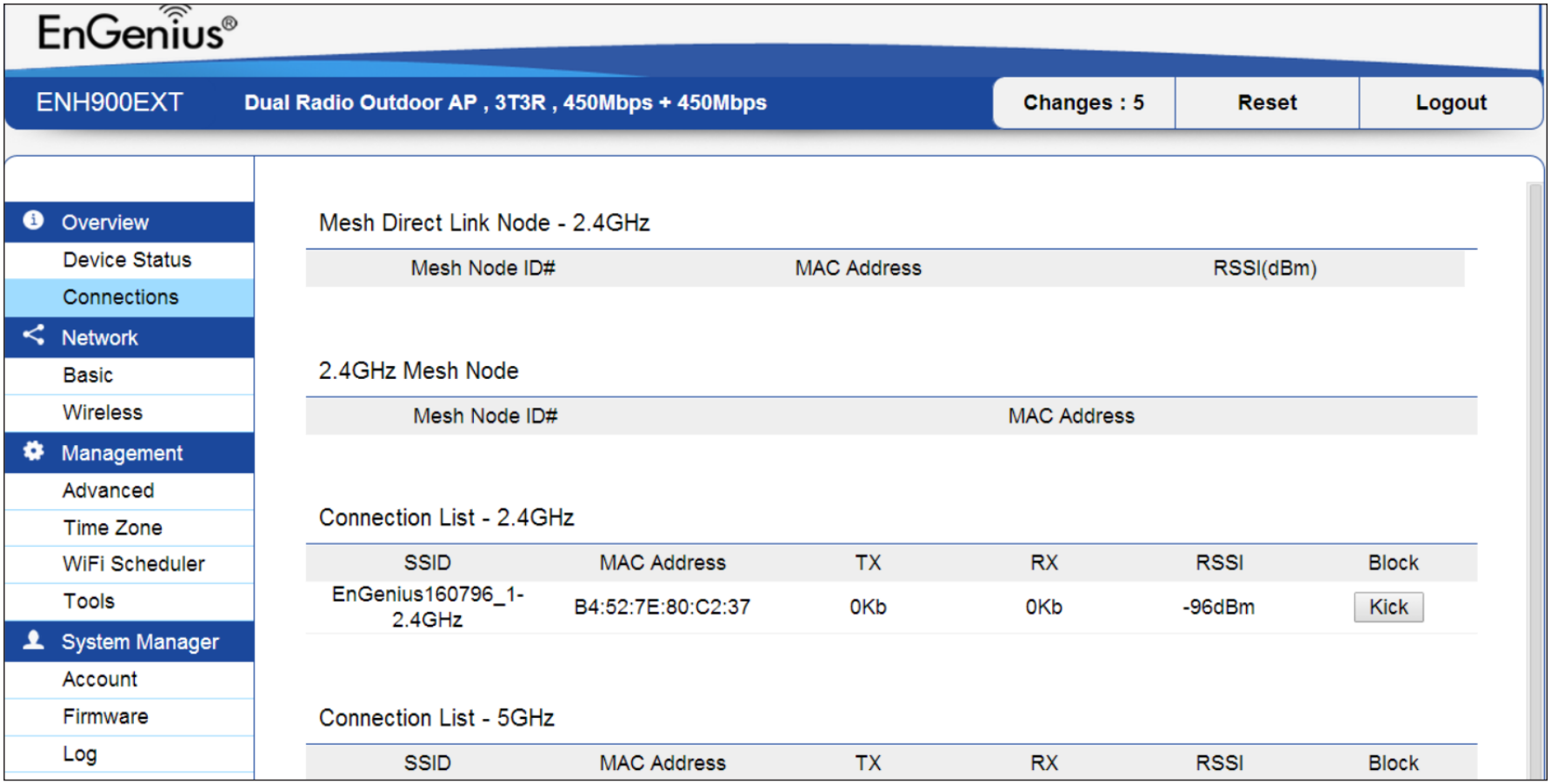
Click the connection link under the Overview menu displays the connection list of clients associated to the ENH900EXT's 2.4 GHz/5 GHz, along with the MAC addresses and signal strength for each client. Clicking **Refresh** updates the client list.

Note: Only applicable in Access Point and WDS AP modes.

2.4 GHz/5 GHz WDS Link List

Click the connection link under the Overview menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

Note: Only applicable in WDS AP and WDS Bridge modes.



The Mesh Link List

Monitor the 2.4GHz Mesh Link List under the status menu. The page will display the current status of the Mesh Links under the Mesh AP mode and Mesh nodes under the Mesh Only mode.

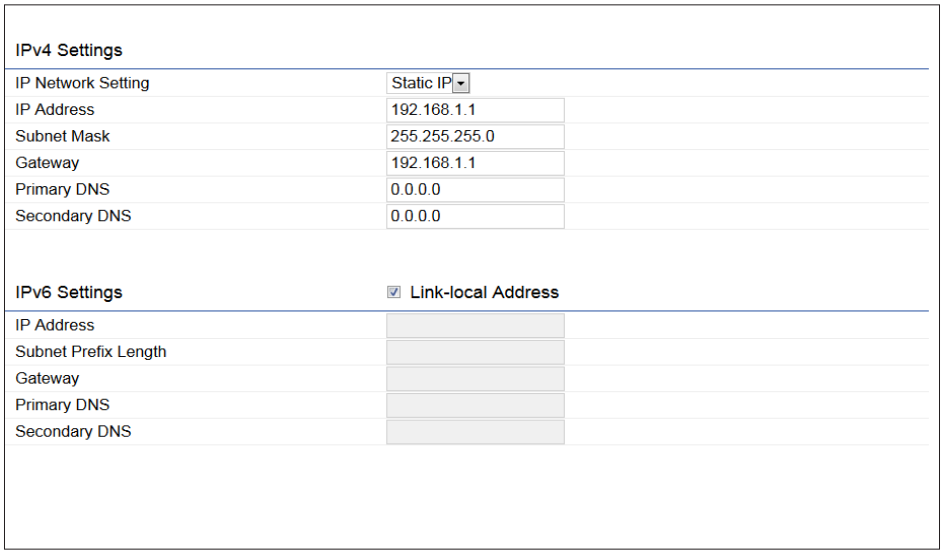
Note: Only Applicable in the Mesh AP and Mesh Only mode.

Chapter 6
Network

Basic IP Settings

IPv4/IPv6 Settings

This page allows you to modify the device's IP settings.



IP Network Settings: Select whether the device IP address will use a static IP address specified in the IP address field or be obtained automatically when the device connects to a DHCP server.

IP Address: The IP address of this device.

Subnet Mask: The IP Subnet mask of this device.

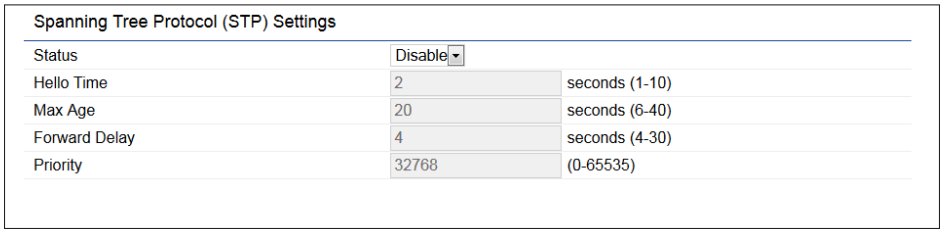
Gateway: The Default Gateway of this device. Leave it blank if you are unsure of this setting.

Primary/Secondary DNS: The primary/secondary DNS address for this device.

Save: Click **Save** to confirm the changes.

Spanning Tree Protocol (STP) Settings

This page allows you to modify the Spanning Tree settings. Enabling the Spanning Tree protocol will prevent network loops in your LAN network.



Spanning Tree Status: Enables or disables the Spanning Tree function.

Hello Time: Specifies Bridge Hello Time in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.

Max Age: Specifies Bridge Max Age in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be inactive.

Forward Delay: Specifies Bridge Forward Delay in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it analyzes data traffic before participating in the network.

Priority: Specifies the Priority Number. A smaller number has a greater priority than a larger number.

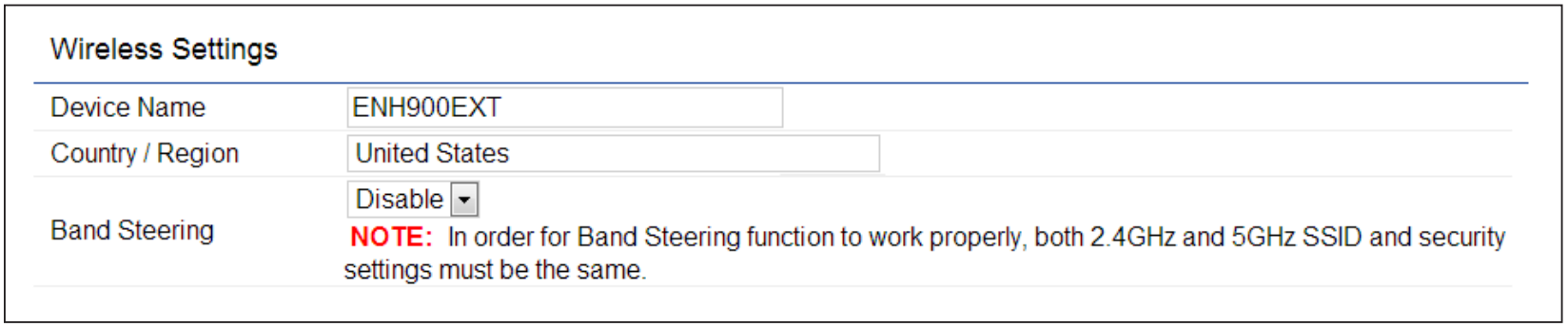
Save: Click **Save** to confirm the changes.

Chapter 7

2.4 GHz & 5 GHz Wireless

Wireless

Wireless Settings


Wireless Settings
Device Name
ENH900EXT
Country / Region
United States
Band Steering
Disable
NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and security settings must be the same.

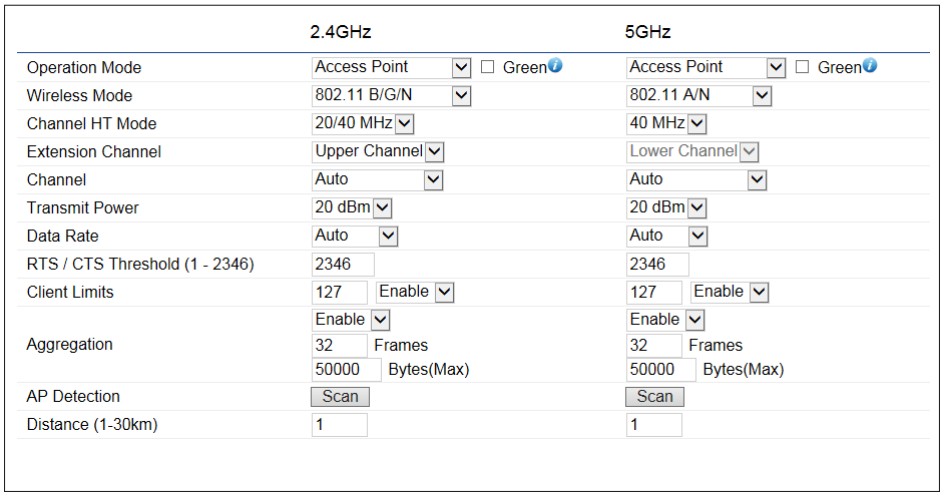
Device Name: Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.

Band Steering: Enable Band Steering to send 802.11n clients to the 5 GHz band, where 802.11b/g clients cannot go, and leave 802.11b/g clients in 2.4GHz to operate at their slower rates. Band Steering works within the Access Point by directing 5 GHz-capable clients to that band.

Save: Click **Save** to confirm the changes.

This page displays the current status of the Wireless settings of the ENH900EXT.

2.4 GHz/5 GHz Wireless Network



Operation Mode: Select **Operation Mode**. The ENH900EXT supports three different operation modes: Access Point, or WDS (WDS AP, WDS Bridge, and WDS Station).

Wireless Mode: Supports 802.11b/g/n mixed mode in 2.4 GHz and 802.11a/n mixed mode in 5 GHz.

Channel HT Mode: The default channel bandwidth is 20 MHz/ 40 MHz. The larger the channel, the greater the transmission quality and speed.

Extension Channel: Select upper or lower channel. Your selection may affect the Auto channel function.

Channel: Select the channel and frequency appropriate for your country's regulation. Select **Auto** to enable auto-channel selection.

Transmit Power: Sets the power output of the wireless signal.

Data Rate: Select a data rate from the drop-down list. The data rate affects throughput of data in the ENH900EXT. Select the best balance for you and your network but note that the lower the data rate, the lower the throughput, though transmission distance is also lowered.

RTS/CTS Threshold: Specifies the threshold package size for RTC/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth.

Client Limits: Limits the total number of clients.

Aggregation: Merges data packets into one packet. This option reduces the number of packets, but also increases packet sizes.

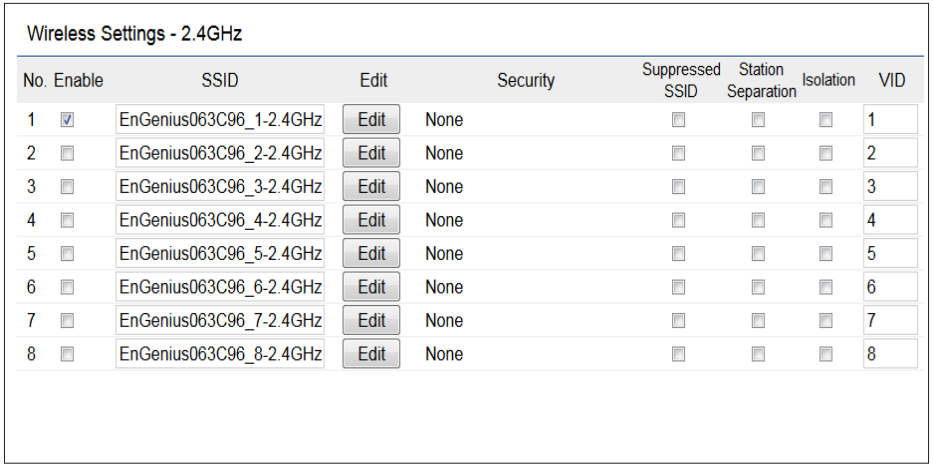
AP Detection: AP Detection can select the best channel to

use by scanning nearby areas for Access Points.

Distance: Specifies the distance between Access Points and clients. Note that longer distances may drop higher-speed connections.

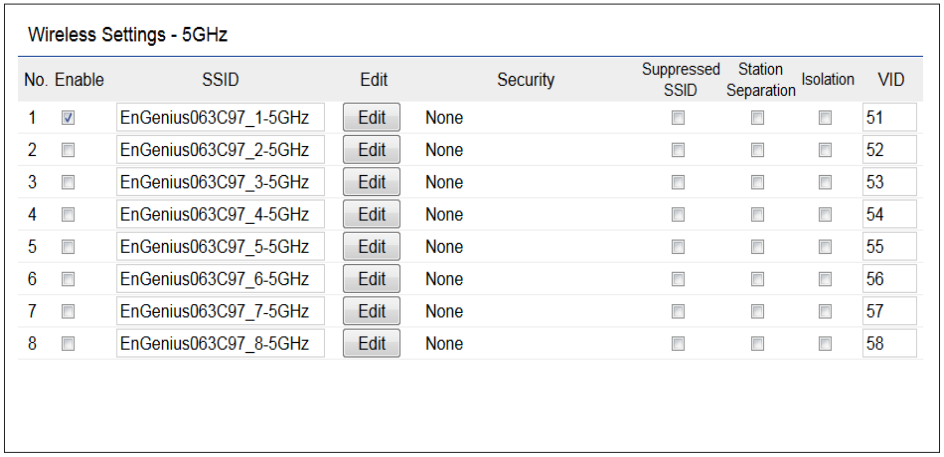
Save: Click **Save** to confirm the changes or **Cancel** to cancel and return to previous settings.

2.4 GHz/5 GHz SSID Profile



Wireless Settings - 2.4GHz

No.	Enable	SSID	Edit	Security	Suppressed SSID	Station Separation	Isolation	VID
1	☑	EnGenius063C96_1-2.4GHz	Edit	None	☐	☐	☐	1
2	☐	EnGenius063C96_2-2.4GHz	Edit	None	☐	☐	☐	2
3	☐	EnGenius063C96_3-2.4GHz	Edit	None	☐	☐	☐	3
4	☐	EnGenius063C96_4-2.4GHz	Edit	None	☐	☐	☐	4
5	☐	EnGenius063C96_5-2.4GHz	Edit	None	☐	☐	☐	5
6	☐	EnGenius063C96_6-2.4GHz	Edit	None	☐	☐	☐	6
7	☐	EnGenius063C96_7-2.4GHz	Edit	None	☐	☐	☐	7
8	☐	EnGenius063C96_8-2.4GHz	Edit	None	☐	☐	☐	8



Wireless Settings - 5GHz

No.	Enable	SSID	Edit	Security	Suppressed SSID	Station Separation	Isolation	VID
1	☑	EnGenius063C97_1-5GHz	Edit	None	☐	☐	☐	51
2	☐	EnGenius063C97_2-5GHz	Edit	None	☐	☐	☐	52
3	☐	EnGenius063C97_3-5GHz	Edit	None	☐	☐	☐	53
4	☐	EnGenius063C97_4-5GHz	Edit	None	☐	☐	☐	54
5	☐	EnGenius063C97_5-5GHz	Edit	None	☐	☐	☐	55
6	☐	EnGenius063C97_6-5GHz	Edit	None	☐	☐	☐	56
7	☐	EnGenius063C97_7-5GHz	Edit	None	☐	☐	☐	57
8	☐	EnGenius063C97_8-5GHz	Edit	None	☐	☐	☐	58

Current Profile: You can configure up to sixteen (16) different SSIDs (eight (8) per band). If multiple client devices will be accessing the network, you can arrange the devices into SSID groups. Click **Edit** to configure the profile and check whether you want to enable extra SSID.

SSID: Specifies the SSID for the current profile.

Suppressed SSID: Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Station Separation: Click the appropriate radio button to allow or prevent communication between client devices.

VID: Specifies the VLAN tag for each profile. If your netowrk includes VLANs, you can specify a VLAN ID for packets pass through the Access Point with a tag.

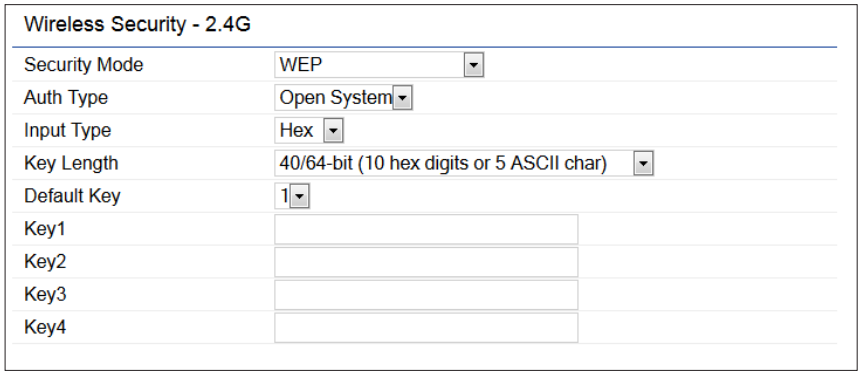
Wireless Security: See the Wireless Security section.

Isolation: Restrict clients communicating with different VIDs by selecting the radio button.

Save: Click **Save** to accept the changes.

Wireless Security

The Wireless Security section lets you configure the ENH900EXT's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. It is strongly recommend that you use WPA2-PSK.



Auth Type: Select **Open System** or **Shared Key**.

Input Type:

ASCII: Regular Text (recommended)

Hexadecimal Numbers (For advanced users)

Key Length: Select the desired option and ensure that wireless clients use the same setting. Your choices are 64, 128, and 152-bit password lengths.

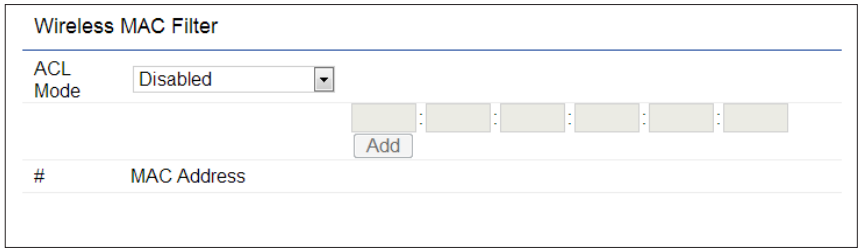
Default Key: Select the Key you wish to be the default. Transmitted data is **ALWAYS** encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key.

Encryption Key Number: Enter the Key Value or values you wish to use. Only the Key selected as Default is required. The others are optional.

Wireless MAC Filtering

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access the ENH900EXT. The default setting is: **Disable Wireless MAC Filter**.

Note: Only applicable in Access Point and WDS AP modes.



ACL Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Your choices are: Disabled, Deny MAC in the list, or Allow MAC in the list.

MAC Address: Enter the MAC address of the wireless client.

Add: Click **Add** to add the MAC address to the MAC address table.

Delete: Delete the selected entries.

Save: Click **Save** to apply the changes.

Wireless Advanced

Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

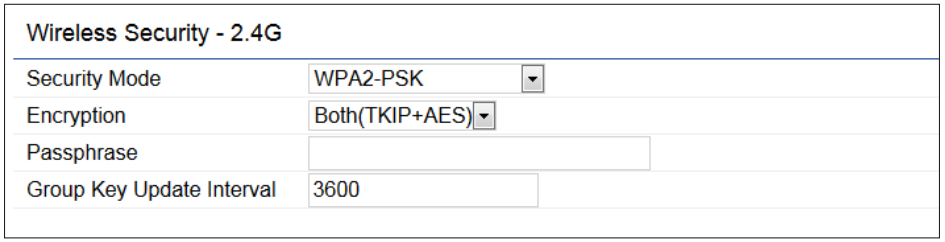
Enable Traffic Shaping: Check this option to enable Wireless Traffic Shaping.

Download Limit: Specifies the wireless transmission speed used for downloading.

Upload Limit: Specifies the wireless transmission speed used for uploading.

Save: Click **Save** to confirm the changes.

WPA-PSK (WPA Pre-Shared Key) Encryption:

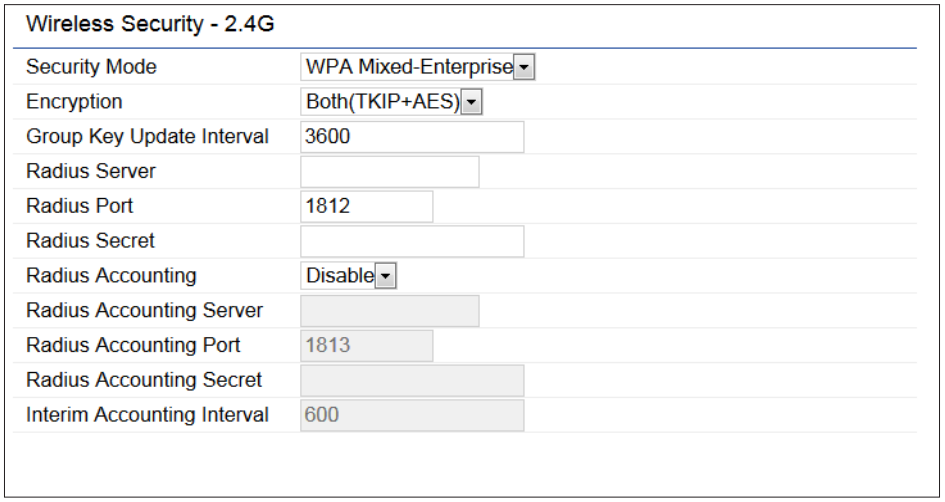


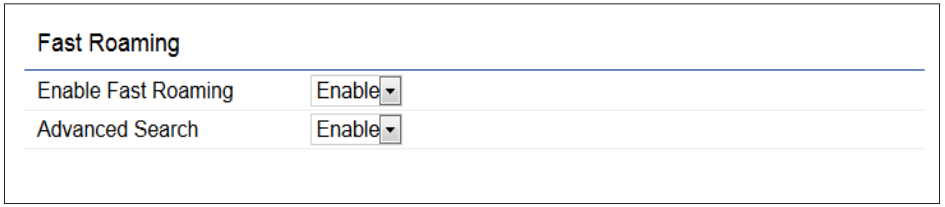
Encryption: Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

Group Key Update Interval: Specifies how often, in seconds, the Group Key changes.

WPA Mixed-Enterprise: Access Point / WDS AP mode





Encryption: Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the port number used for connections to the Radius server.

Radius Secret: Enter the secret required to connect to the Radius server.

Group Key Update Interval: Specifies how often, in seconds, the Group Key changes.

Radius Accounting: Enable or disable accounting feature.

Radius Accounting Server: Enter the IP address of the Radius accounting server.

Radius Accounting Port Enter the port number used for connections to the Radius accounting server.

Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

Interim Accounting Interval: Specifies how often, in seconds, the accounting data sends.

> **Note:** 802.11n does not allow WEP/WPA-PSK TKIP/ WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

Fast Roaming: Enable Fast Roaming to serve mobile client devices that roam from Access Point to Access Point. Some applications running on Client devices require fast re-association when they roam to a different Access Point. Voice application, for example, requires seamless roaming to prevent delays in conversations.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

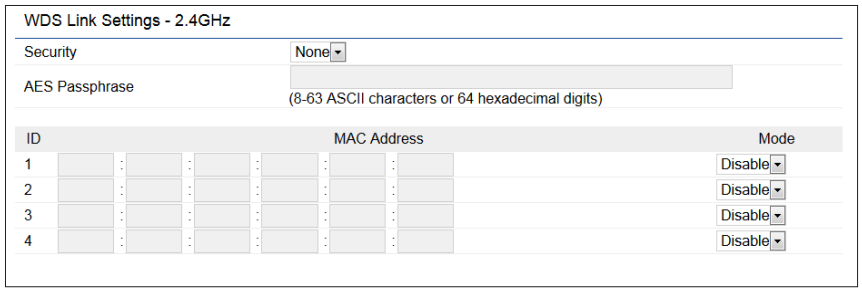
Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

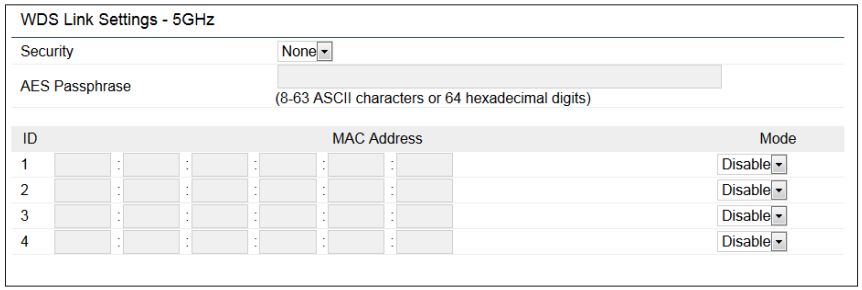
Also note: All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four Access Points.

Note: Only applicable in WDS AP and WDS Bridge modes.

2.4 GHz/5 GHz WDS Link Settings





Security: Select **None** or **AES** from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

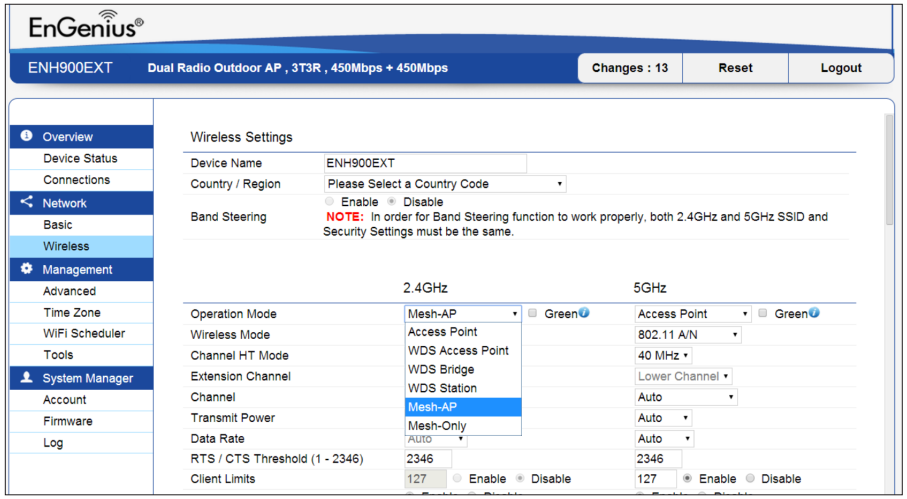
Mode: Select to disable or enable from the drop-down list.

Save: Click **Save** to confirm the changes.

2.4 GHz Mesh Link Settings

Users can choose the 2.4 GHz band for Mesh operation.

Mesh Settings



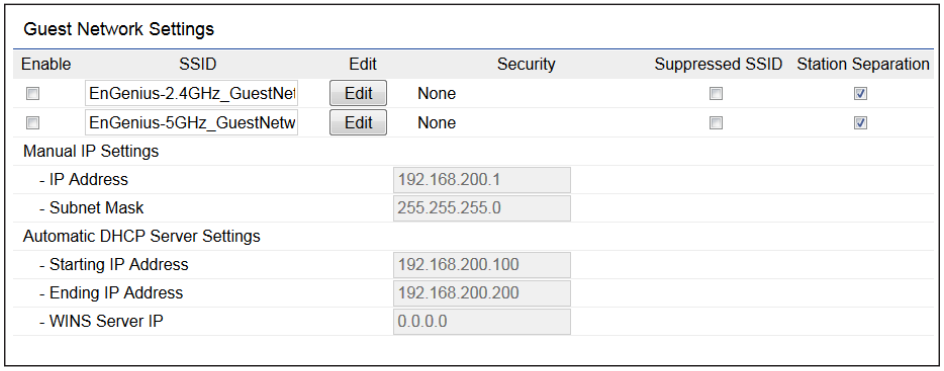
Mesh SSID: To create a mesh network, please enter the Mesh SSID of the Access Point that you wish to include in the Mesh.

Security: Select None or WPA2-PSK AES from drop-down list.

AES Passphrase: Enter the key values you wish to uses. Other Access Points must use the same key to establish a mesh link

Guest Network Settings

Adding a guest network allows visitors to use the Internet without giving out your office or company wireless security key. You can add a guest network to each wireless network in the 2.4 GHzb/g/n and 5 GHza/n frequencies.



SSID: Specifies the SSID for the current profile.

Suppressed SSID: Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Station Separation: Click the appropriate radio button to allow or prevent communication between client devices.

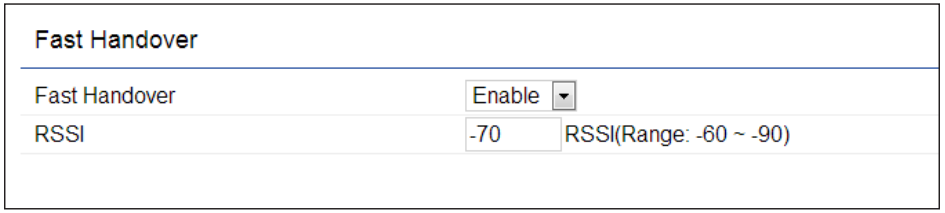
IP Address: The IP Address of this device.

Subnet Mask: The IP Subnet mask of this device.

Starting IP Address: The first IP Address in the range of the addresses by the DHCP server.

Ending IP Address: The last IP Address in the range of addresses assigned by the DHCP server.

Fast Handover



Fast Handover: Enable the Fast Handover feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vincinity of that client to coordinate which of them should serve the client best.

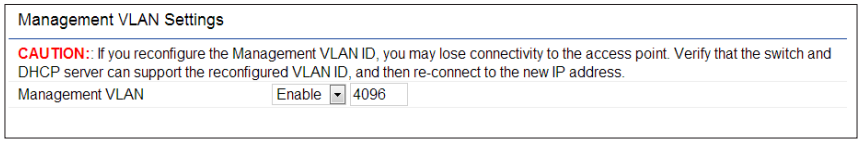
RSSI: Enter the RSSI (Received Signal Strength Index) in order to determine the handover procedure which the current wireless link will terminate. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.

Chapter 8
Management

Management VLAN Settings

This page allows you to assign a VLAN tag to packets sent over the network. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Note: Only applicable in Access Point and WDS AP modes.


Management VLAN Settings
CAUTION:: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.
Management VLAN
Enable
4096

Management VLAN: If your network includes VLANs, you can enable **Management VLAN ID** for packets passing through the Access Point with a tag.

Save: Click **Save** to confirm the changes or **Cancel** to cancel and return to previous settings.

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the ENH900EXT. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the ENH900EXT using the new IP address.

Wi-Fi Multi Media (WMM)

This feature provide QoS (Quality of Service) for prioritizing multimedia traffic on the network. WMM prioritization achieves the goal of minimizing delay in a wireless network for time-sensitive applications such as video streaming.

WMM Parameters	CWmin	CWmax	AIFS	TXOPlimit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

WMM Parameters: According to version 1.1 of the WMM specifications by the Wi-Fi Alliance, defines four Access Category (AC_BE, AC_BK, AC_VI, AC_VO) labels in order to provide more favorable network access for applications that are less tolerant of packet delays.

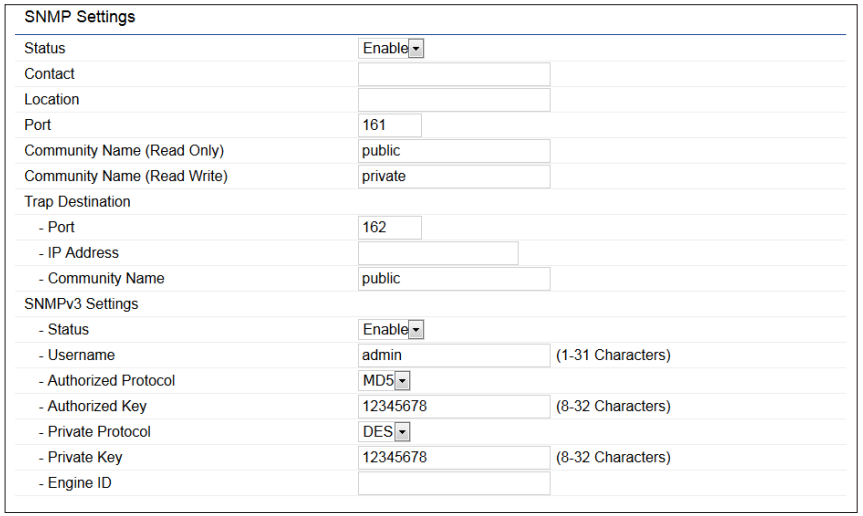
CW: CW (Contention Window) maintains the DCF random back-off component to help avoid collisions of packets from the same access category.

AIFS: Arbitration Inter-Frame Spacing (AIFS) in wireless LAN communications is a method of prioritizing one Access Class (AC) over the other, such as giving voice or video priority over email.

Advanced Settings

SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for a Simple Network Management Protocol (SNMP). SNMP is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) returns the data stored in their Management Information Bases.



SNMP Enable/Disable: Enables or disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device.

Community Name (Read Only): Specifies the password for the SNMP community for read only access.

Community Name (Read/Write): Specifies the password for the SNMP community with read/write access.

Trap Destination Address: Specifies the IP address of the computer that will receive the SNMP traps.

Trap Destination Community Name: Specifies the password for the SNMP trap community.

SNMPv3: Enables or disables the SNMPv3 feature.

User Name: Specifies the username for SNMPv3.

Auth Protocol: Selects the authentication protocol type: MDS or SHA.

Auth Key: Specifies the authentication key.

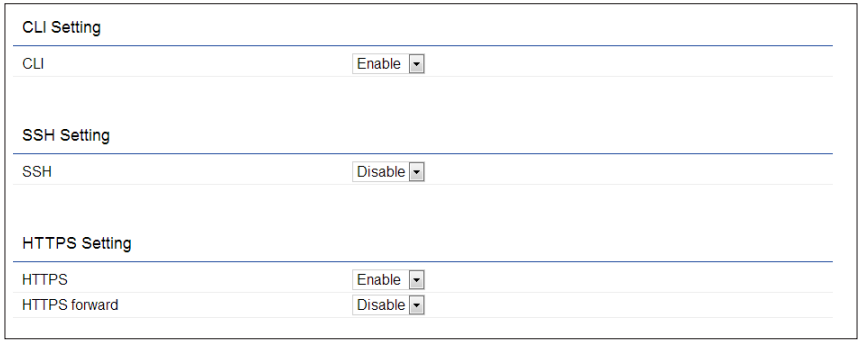
Priv Protocol: Selects the privacy protocol type: DES.

Priv Key: Specifies the privacy key for privacy.

Engine ID: Specifies the engine ID for SNMPv3.

Apply Save: Click **Apply Save** to apply the changes.

CLI Settings



CLI: The Command Line Interface (CLI) allows you to type commands instead of choosing them from a menu or selecting an icon.

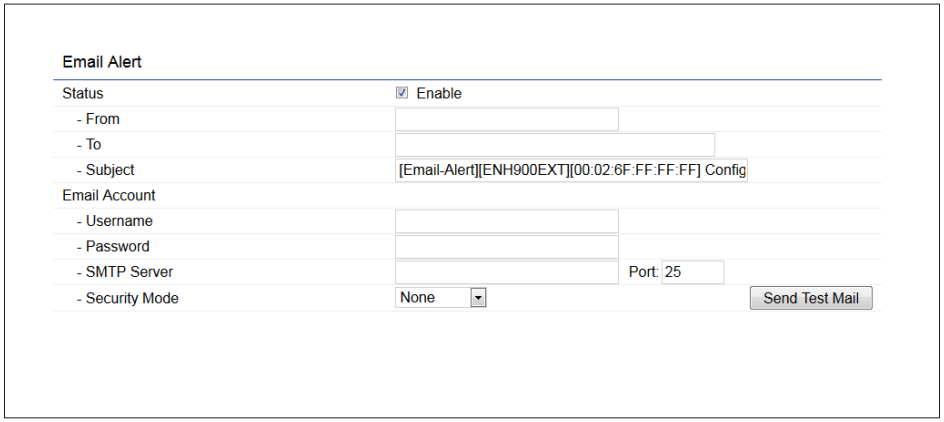
SSH: Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.

HTTPS: Enable HTTPS to transfer and display web content securely. The Hypertext Transfer Protocol over SSL (Secure Socket Layer) is a TCP/IP protocol used by web servers to transfer and display web content securely.

Email Alert

You can use the Email Alert feature to send messages to the configured email address when particular system events occur.

Note: Do **NOT** use your personal email address as it can unnecessarily expose your personal email login credentials. Use a separate email account made for this feature instead



From: Enter the email address to show the sender of the email.

To: Enter the address to receive email alerts.

Subject: Enter the text to appear in the email subject line.

Username: Enter the username for the email account that will be used to send emails.

Password: Enter the password for the email account that will be used to send emails.

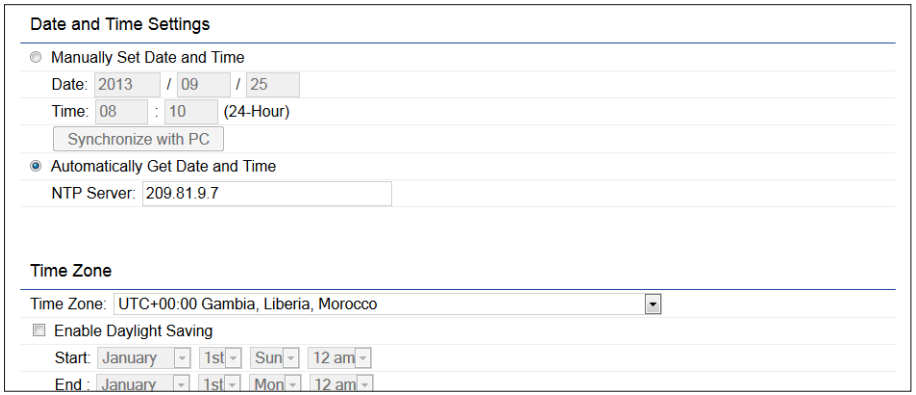
SMTP Server: Enter the IP address or hostname of the outgoing SMTP server.

Port: Enter the SMTP port number to use for outbound emails.

Time Zone

Time Setting

This page allows you to set the internal clock of the ENH900EXT.


Date and Time Settings
Manually Set Date and Time
Date: 2013 / 09 / 25
Time: 08 : 10 (24-Hour)
Synchronize with PC
Automatically Get Date and Time
NTP Server: 209.81.9.7
Time Zone
Time Zone: UTC+00:00 Gambia, Liberia, Morocco
Enable Daylight Saving
Start: January 1st Sun 12 am
End : January 1st Mon 12 am

Manually Set Date and Time: Manually specify the date and time.

Automatically Get Date and Time: Select **Automatically Get Date and Time** and check whether you wish to enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.

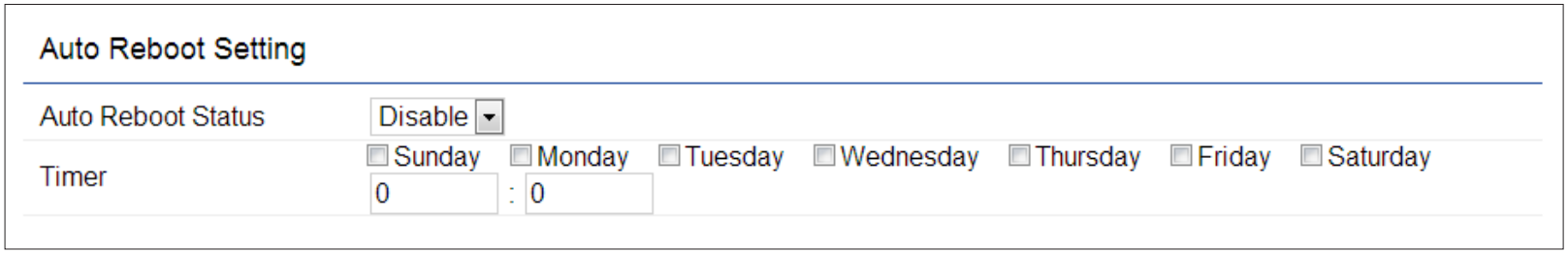
Enable Daylight Saving: Check whether daylight savings applies to your area.

Start: Select the day, month, and time when daylight savings time starts.

End: Select the day, month, and time when daylight savings times ends.

Auto Reboot Settings

You can specify how often you wish to reboot the ENH900EXT.



Auto Reboot Setting: Enables or disables the Auto Reboot function.

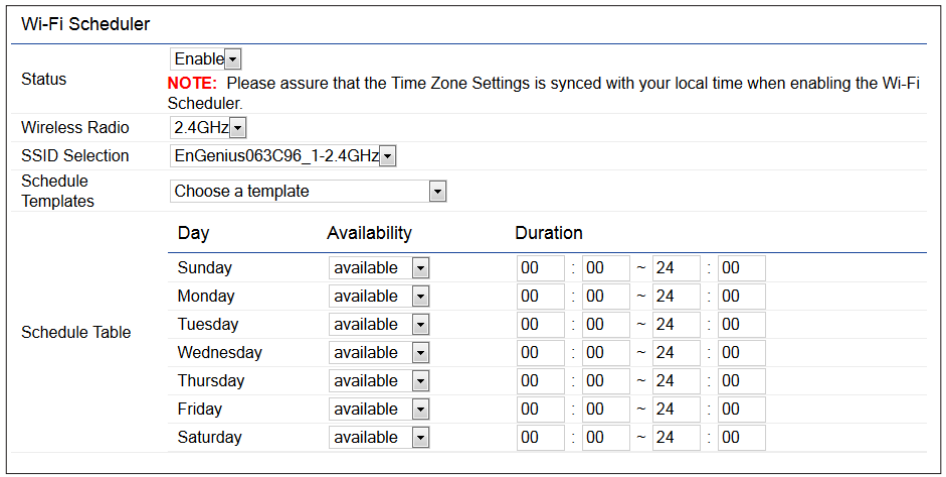
Frequency of Auto Reboot: Specifies how often you wish to reboot the ENH900EXT by Min, Hour, Day or Week.

Timer: Select the day and enter the time you would like to reboot automatically.

Save: Click **Save** to apply the changes.

Wi-Fi Scheduler

The Wi-Fi Scheduler can be created for use in enforcing rules. For example, if you wish to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu and Fri while entering a Start time of 3pm and End Time of 8pm to limit access to these times.



Status: Enables or disables the Wi-Fi scheduler function.

Wireless Radio: Select 2.4 GHz or 5 GHz from the drop-down list for the preferred band type.

SSID Selection: Select a SSID from the drop-down list.

Schedule Templates: Select a schedule template from the drop-down list.

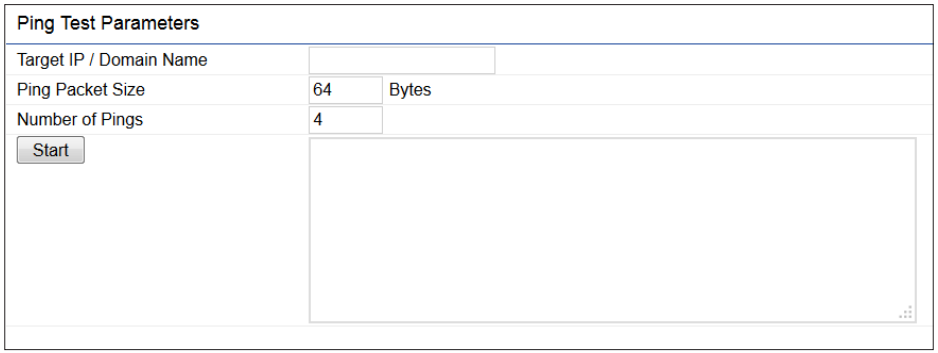
Day(s): Place a checkmark in the boxes for the desired days or select the **All Week** radio button to select all seven days of the week.

Duration: The Start Time is entered in two fields. The first box is for hours and the second box is for minutes. The End Time is entered in the same format as the Start time.

Tools

Ping Test Parameters

This page allows you to analyze the connection quality of the ENH900EXT and trace the routing table to a target in the network.



Target IP: Enter the IP address you would like to search.

Ping Packet Size: Enter the packet size of each ping.

Number of Pings: Enter the number of times you wish to ping.

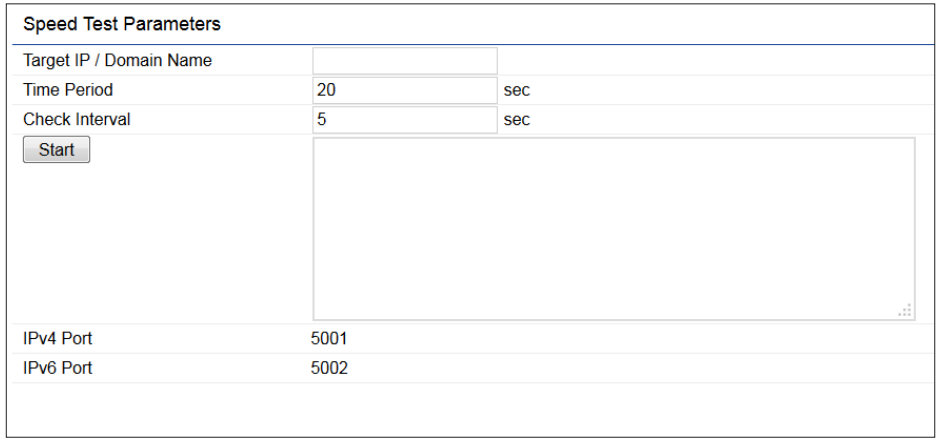
Start Ping: Click **Start Ping** to begin pinging the target device (via IP).

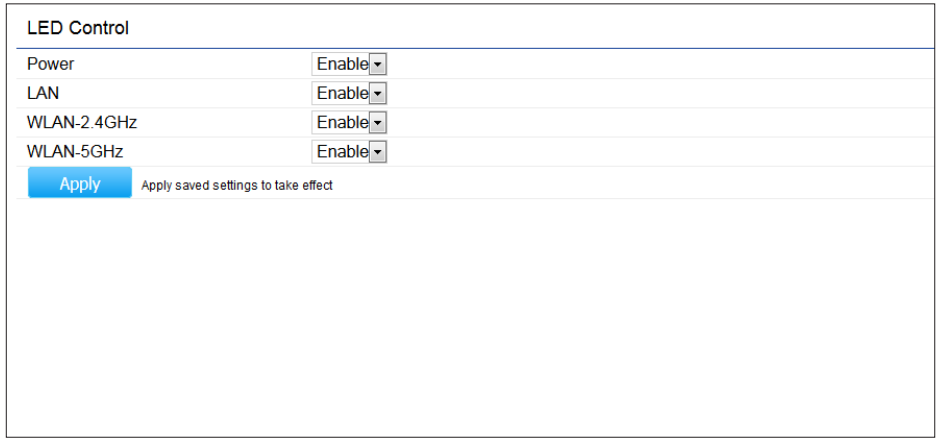
Traceroute Target: Enter the IP address or domain name you wish to trace.

Start Traceroute: Click **Start Traceroute** to begin the trace route operation.

Speed Test Parameters / LED Control

This page allows you to control LED on/off for Power, LAN interface, or 2.4 GHz/5 GHz WLAN interface.





LED Control

Power: Enables or disables the Power LED indicator.

LAN: Enables or disables the LAN LED indicator.

WLAN-2.4 GHz: Enables or disables the WLAN-2.4 GHz LED indicator.

WLAN-5 GHz: Enables or disables the WLAN-5 GHz LED indicator.

Device Discovery

This page allows you to discover devices from network for Operation Mode, IP Address, System MAC Address and Firmware version.

Account

This page allows you to change the ENH900EXT username and password. By default, the username is: **admin** and the password is: **admin**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.

Account Settings

Administrator Username: Enter a new username for logging in to the New Name entry box.

Current Password: Enter the old password for logging in to the Old Password entry box.

New Password: Enter the new password for logging in to the New Password entry box.

Verify Password: Re-enter the new password in the Confirm Password entry box for confirmation.

Apply: Click **Apply** to apply the changes.

Firmware

Firmware Upgrade

This page allows you to upgrade the firmware of the ENH900EXT.

To Perform the Firmware Upgrade:

1. Click the **Choose File** button and navigate the OS file system to the location of the upgrade file.
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the **Upload** button to commence the firmware upgrade.

   Note: The device is unavailable during the Firmware upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

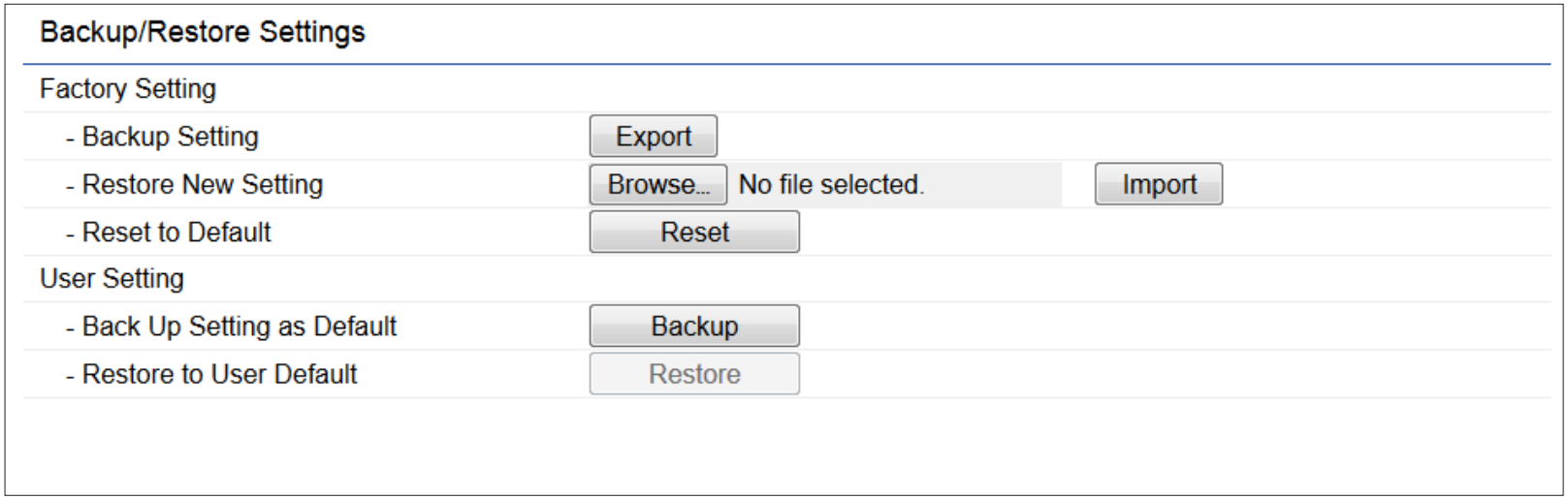
Backup/Restore

This page allows you to save the current device configurations. When you save your configurations, you also can reload the saved configurations into the device through the Restore Saved Settings from a file section. If extreme problems occur, or if you have set the ENH900EXT incorrectly, you can use the **Reset** button in the Revert to Factory Default Settings section to restore all the configurations of the ENH900EXT to the original default settings.

Backup Setting: Click **Export** to save the current configured settings.

Restore New Setting: To restore settings that have been previously backed up, click **Browse**, select the file, and click **Restore**.

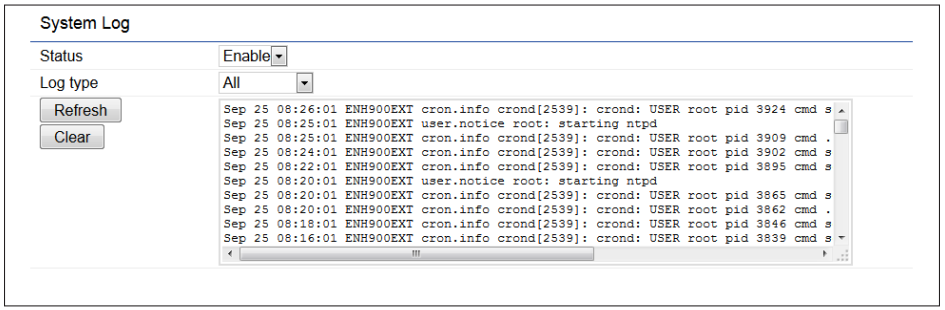
Restore to Default: Click **Reset** button to restore the ENH900EXT to its factory default settings.



Log

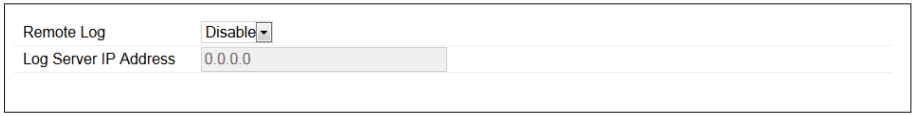
System Log

The ENH900EXT automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **Log** link under the System Manager menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.


System Log
Status
Enable
Log type
All
Refresh
Clear
Sep 25 08:26:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3924 cmd s
Sep 25 08:25:01 ENH900EXT user.notice root: starting ntpd
Sep 25 08:25:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3909 cmd .
Sep 25 08:24:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3902 cmd s
Sep 25 08:22:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3895 cmd s
Sep 25 08:20:01 ENH900EXT user.notice root: starting ntpd
Sep 25 08:20:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3865 cmd s
Sep 25 08:20:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3862 cmd .
Sep 25 08:18:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3846 cmd s
Sep 25 08:16:01 ENH900EXT cron.info crond[2539]: crond: USER root pid 3839 cmd s

Remote Log

This page allows you to setup the Remote Log functions for the ENH900EXT.



Syslog: Enables or disables the syslog function.

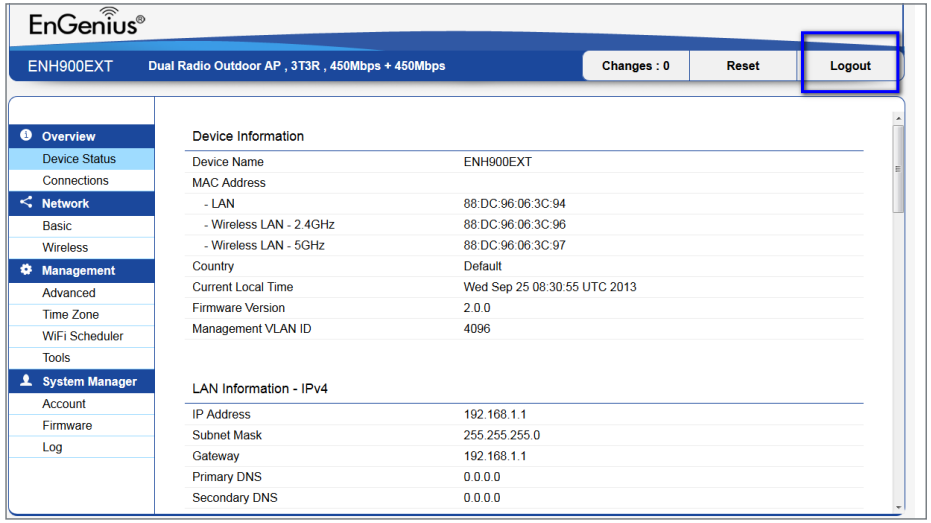
Log Server IP Address: Enter the IP address of the log server.

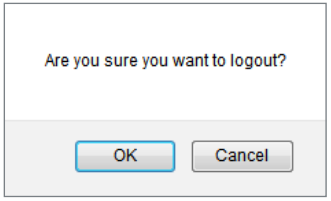
Remote Log: Enable or disable the remote log service.

Apply: Click **Apply** to apply the changes.

Logout

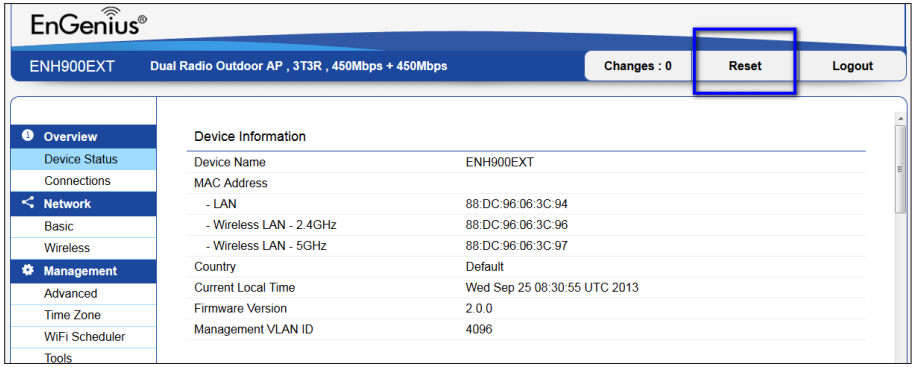
Click **Logout** in Management menu to logout.

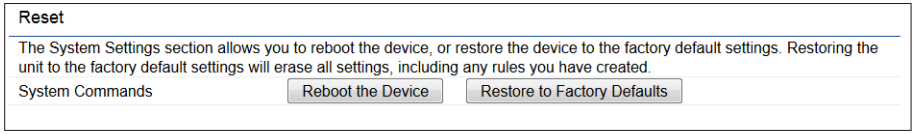




Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reset** to reboot the ENH900EXT.




Reset
The System Settings section allows you to reboot the device, or restore the device to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules you have created.
System Commands
Reboot the Device
Restore to Factory Defaults

Glossary

6to4	6to4 allows IPv6 packets to be transmitted over an IPv4 network.
ACL	The Access Control List specifies which users or processes are granted access to objects, as well as which operations are allowed.
Access Point Mode	In Access Point mode, the EPG600 allows wireless devices to connect to a wired network using Wi-Fi, or other related standards. You can choose to have the router associate only with certain iterations (IEEE standards) and by doing so this will either positively or negatively affect the router's speed and throughput performance.
AES	An Advanced Encryption Standard is an encryption algorithm. You can chose 128, 192 or 256-bit long key size for encryption and decryption of text.
ALG	Application Layer Gateway serves as a window between correspondent application processes so that they may exchange information on an open environment.
Backup	A copy of a set of files made for replacement purposes in case the original set is damaged or lost.
Bandwidth	Bandwidth refers to the information-carrying capacity of a network or component of a network expressed in bits per second.
Bit Rate	The rate at which bits are transmitted or received during communication, expressed as the number bits in a given amount of time, usually one second.
Boot	A computer's startup operation.
Community String	A text string that acts as a password and is used to authenticate messages sent between a management station and a router containing a SNMP agent. The community string is sent in every packet between the manager and the agent.
Default Gateway	A Deafult Gateway is the device that passes traffic from the local subnet to devices on other subnets. It is usually the IP address of the router to which your network is connected.
DES	A Data Encryption Standard is an encryption type that enhances the encryption capabilities of SNMP version 3.
DDNS	Dynamic Domain Name Service (DDNS) allows for an Internet domain name to be assigned to a computer with a varying (dynamic) IP address.
DHCP	The Dynamic Host Cnfiguation protocol is used for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
DLNA	The Digital Living Network Alliance DLNA is a nonprofit collaborative trade organization that is responsible for defining interoperability guidelines to enable the sharing of digital media between multimedia devices. Some HDTVs, Gaming Consoles, and other media devices adhere to DLNA guidelines.

DNS	A Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. This allows the recognition of domain names such as www.yahoo.com instead of 98.139.183.24, which is more difficult to remember.
Domain	A portion of the spanning hierarchy tree that refers to general groupings of networks based on organization type or geography.
DoS	Denial of Service is an interruption in an authorized user's access to a computer network and is typically caused with malicious intent. Although the process and targets of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to a network.
Download	The transfer of a file from a remote computer to a local computer.
Dynamic IP	An IP address that is assigned and changed periodically. Dynamic IP addresses can change each time you connect to the Internet, while static IP addresses are reserved for you statically and don't change over time.
Encryption	The application of a specific algorithm to data so as to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.
Firewall	A router or access server, or several routers or access servers designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
Firmware	A collection of programmed routines and instructions that is implemented in a computer chip or similar hardware form instead of a software form. Please check www.engeniustech.com for firmware updates.
FTP	An application protocol that uses the TCP/IP protocols. It is used to exchange files between computers/devices on networks.
Gateway	A gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway,and a Switch, which furnishes the actual path in and out of the gateway for a given packet.
Guest Network	A guest network is a section of an computer network designed for use by temporary visitors. This subnetwork often provides full Internet connectivity, but also strictly limits access to any internal Web sites or files.

GUI	Graphical User Interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored.
IGMP	The Internet Group Multicast Protocol is a protocol that provides the means for a host to inform its attached router that an application running wants to join a specific multicast group.
IP	The Internet Protocol is a method transmitting data over a network. Data to be sent is divided into individual and completely independent "packets." Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender's address and the receiver's address. The Internet Protocol ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, (which means that there is no established connection between the communication endpoints) packets can be sent via different routes and do not need to arrive at the destination in the correct order. Once the data packets have arrived at the correct destination, another protocol, Transmission Control Protocol (TCP) puts them in the right order.
IP Address	An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and to pass data back and forth. To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed, so that it does not change, or it can be assigned dynamically (and automatically) by DHCP. An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. One part represent the network number or address, and other part represents the local machine address.
IPv6	IPv6 provides an identification and location system for computers on networks and routes that traffic across the Internet.
L2TP	The Layer 2 Tunneling Protocol is used to support VPNs or as part of the delivery of services by ISPs.
LAN	A communication infrastructure that supports data and resource sharing within a small area that is completely contained on the premises of a single owner.
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.
MAC Address Filtering	Mac Address Filtering permits and denies network access to specific devices based on a device's MAC address.
MD5	A Message-Digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number.

Mesh Mode	Mesh Networks are a network topology in which each node (called a mesh node) relays data for the network. All nodes cooperate in the distribution of data in the network. In the event that a node fails, other nodes can automatically reconfigure or "fill in" for another Wireless AP in the network (called Self-healing) and pickup a signal that otherwise would have been dropped.
MTU	Maximum Transmission Unit. A specification in a data link protocol that defines the maximum number of bytes that can be carried in any one packet on that link.
NAT	Network Address Translation is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NTP Sevrer	The Network Time Protocol is used for clock synchronization between computer systems.
Packet	A discrete chunk of communication in a pre-defined format.
Port Forwarding	Port Forwarding allows remote computers to connect to a specific computer or service within a private LAN.
Port Mapping	Port Mapping allows you to redirect a particular range of service port numbers from the WAN to a particular LAN IP address.
Port Triggering	Port Triggering lets you map a local port or range of ports to a specific public port. Sending packets out over the local port triggers the router to open an incoming local port that is mapped to the same public port and application as the outgoing local port(s). The local application can communicate over the incoming and outgoing ports without the need for creating a fixed address.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. PPPoE can be used to have an office or building-full of users share a common DSL, cable modem, or wireless connection to the Internet.
PPTP	A protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. In this way a corporation can effectively use a WAN as a large single LAN.
Priority Queue	A Priority queue is a queue where an element with a high priority is served before an element with low priority. If two elements happen to have the same priority, they are served according to their order in the queue.
QoS	Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. It is espcially important for applications like multimedia streaming and VoIP.
RADIUS	Remote Authentication Dial In User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for users that connect and use a network service.

RAM	Random Access Memory. A group of memory locations that are numerically identified to allow high speed access by a CPU. In random access, any memory location can be accessed at any time by referring to its numerical identifier as compared to sequential access, where memory location 6 can only be accessed after accessing memory locations 1-5.
Reboot	A user activity where the user starts a computing device without interrupting its source of electrical power.
Router	A device that determines the next network point to which a packet should be forwarded to on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network Switch.
Server	In general, a server is a computer program that provides services to other computer programs within the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. A web server is the computer program that supplies the requested HTML pages or files to the client (browser).
SHA	A Secure Hash Algorithm produces a 160-bit (20-byte) hash value typically rendered as a hexadecimal number, 40 digits long.
Static IP	An IP address that is unchanging. It is more reliable when dealing with VoIP, online gaming, and VPNs.
SSID	A Service Set Identifier is a set consisting of all the devices associated with a WLAN.
Subnet Mask	A representation of a user's Internet address where all of the bit positions corresponding to the user's network and subnetwork id are 1's and the bit corresponding to the user's host id are 0's.
Throughput	Rate of information arriving at, and possibly passing through, a particular point in a network system.
Time-Out	Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. The resulting time-out usually results in a re-transmission of information or the dissolving of the session between the two devices.
TKIP	Temporal Key Integrity Protocol is a stopgap security protocol used in IEEE 802.11 wireless networking standards used to replace WEP.
UID	A Unique Identifier is a unique reference number used as an identifier.
Upload	The activity of transferring a file from a user's computer system to a remote system.
UPnP	Universal Plug n Play is a protocol that permits networked devices to seamlessly discover each other's presence on the network.

VLAN	A Virtual Local Area network allows a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together.
VoIP	Voice over IP is a technology used for the delivery of voice communications and multimedia sessions over IP networks rather than a PSTN line.
VPN	A Virtual Private Network creates a secure “tunnel” between the points within the VPN. Only devices with the correct “key” will be able to work within the VPN. The VPN network can be within a company LAN (Local Area Network), but different sites can also be connected over the Internet in a secure way. One common use for VPN is for connecting a remote computer to the corporate network, via e.g. a direct phone line or the Internet.
VPN Tunnel	VPN Tunneling is a link which connects a network directly to another network. The connection between the complementary links is called a VPN tunnel VPN comprises with a VPN server and a VPN client. A VPN client is usually a software program which can be configured to the VPN server.
WAN	A Wide Area Network is a network that covers a broad area over long distances using private or public network transports between different LANs, MANs and other localised computer networking architectures.
WDS Mode	Wireless Distribution System Mode is a MAC address-based system enabling the wireless interconnection of Access Points in an IEEE 802.11 network.
WEP	Wired Equivalent Privacy is a is a security protocol for wireless networks that encrypts transmitted data.
WLAN	A Wireless LAN is a LAN that links two or more devices using some wireless distribution method. This gives users the ability to move around within a local coverage area and still be connected to the network.
WOL	Wake on LAN allows a computer to be turned on or awakened by a network message.
WPA /WPA2	Wi-Fi Protected Access and Wi-Fi Protected Access II are security protocols and security certification programs used to secure wireless computer networks. They are reccomended over WEP.

Appendix

Appendix A

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

IMPORTANT NOTE:
Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Appendix B - CE Interference Statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**
  Safety of Information Technology Equipment
- **EN50385**
  Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 893**
  Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 489-1**
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560 !

Česky [Czech]	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede [fabrikantens navn] erklærer herved, at følgende udstyr [udstyrets typebetegnelse] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt [Name des Herstellers], dass sich das Gerät [Gerätetyp] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab [tootja nimi = name of manufacturer] seadme [seadme tüüp = type of equipment] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, [name of manufacturer], declares that this [type of equipment] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente [nombre del fabricante] declara que el [clase de equipo] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [name of manufacturer] ΔΗΛΩΝΕΙ ΟΤΙ [type of equipment] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente [nom du fabricant] déclare que l'appareil [type d'appareil] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente [nome del costruttore] dichiara che questo [tipo di apparecchio] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [name of manufacturer / izgatavotāja nosaukums] deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/ 5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [manufacturer name] deklaruoja, kad šis [equipment type] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart [naam van de fabrikant] dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, [isem tal-manifattur], jiddikjara li dan [il-mudel tal-prodott] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, [gyártó neve] nyilatkozom, hogy a [... típus] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym [nazwa producenta] oświadcza, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar [företag] att denna [utrustningstyp] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.